

Tel Aviv University

**The Annual Cyber Security
International Conference
Proceedings 2012-2013**

**The Yuval Ne'eman
Workshop for Science,
Technology and Security**

September 2014

The Annual Cyber Security International Conference Proceedings 2012-2013

Edited By: Lior Tabansky

Yuval Ne'eman Workshop for Science, Technology, and Security was launched in 2002 by Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program with the intention of exploring the link among security policy, technology and science. For this reason the workshop holds an annual series of conferences and conducts research. The workshop covers various topics such as international relations and strategy, missiles and guided weapon, robotics, space policy and security, cyberspace and cyber warfare, nuclear energy, homeland security, the interplay between society and security, force build up policy and government decision-making processes.

Yuval Ne'eman Workshop for Science, Technology, and Security officials:

Major Gen. (Ret.) Prof. Isaac Ben-Israel, Head of the Workshop

Ms. Gili Drob - Heistein, Executive Director of the Workshop

Ms. Revital Yaron

Researches (alphabetical order): Dr. Haim Assa, Gil Baram, Prof. Isaac Ben-Israel, Tal Dekel, Gadi Evron, Adv. Deborah Housen-Couriel, Ram Levi, Dr. Deganit Paikowsky, Uri Rechav, Dr. Martin Sherman, Lior Tabansky, Dr. Roey Tzezana

Graphic Editing: Stav Axenfeld

Printed by: Tel-Aviv University Press, Israel, 2014

© All rights reserved.

<http://sectech.tau.ac.il>

Interdisciplinary Cyber Research Center (ICRC)

Background

The developments of computers over the last fifty years and their penetration into all aspects of our lives have brought, along with a tremendous growth of efficiency, also a weak point. Modern society, computerized to the hilt, has become dependent on computers and is vulnerable to disruptions to their functioning.

The cyber threat, which has earned itself a place in the international consciousness in the last five years, demands special preparations on a state level. These preparations must be made in the security field, as well as the others fields including academia. The cyber dimension penetrates all aspects of our lives, and understanding this requires a mastery of not only the natural disciplines – such as computer sciences, mathematics and engineering – but also of social and legal aspects, and even business and philosophy.

ICRC

On April 2014, we established at Tel Aviv University, an Interdisciplinary Cyber Studies and Research Center. The Center was founded on a joint initiative with the National Cyber Bureau, Prime Minister Office.

The Center established on the basis of researchers at the University in various cyber fields, and deals with the interdisciplinary study and research of cyber. The Center aims to become a leading international body in the field, and to increase the academic efforts and awareness in the field of cyber security. In areas where there is presently a lack of researchers, the Center will work to create suitable knowledge-centers in the University and will in the meantime rely on joint research with other knowledge-centers in Israel.

Research issues will include core issues (such as: software security, attacks on hardware and software, cryptography, network protocols, operating system security, networks, etc.) along with interdisciplinary issues (such as: influencing national security, cyber and society, regulatory issues, influencing the business sector, etc.).

Table of Contents

Opening remarks

Head of Yuval Ne’eman Workshop for Science, Technology and Security 9

Executive Director of Yuval Ne’eman Workshop for Science, Technology and Security..... 10

Yuval Ne’eman Workshop’s 2nd Annual International Conference on: Cyber Security - 2012:

Conference Agenda 12

Opening Session

Prof. Maj. Gen. (Res.) Isaac Ben Israel, Head of Yuval Ne’eman Workshop for Science, Technology and Security 14

Prof. Joseph Klafter, President of Tel Aviv University..... 15

Mr. Ehud Barak, Israel’s Minister of Defense 17

Dr. Eviatar Matania, Head of the National Cyber Bureau, Prime Minister’s Office 20

First Session:

From Information Security to Cyber Security

Uncovering Invisible Threats

Mr. Robert Shaw, President and CEO, Net Optics 24

Cyber Trends, Futures, and Road Map To Enhanced Security

Mr. Curt Aubley, VP/CTO Cyber Security & NexGen Innovation, Lockheed Martin 28

Social Networks Security

Prof. Yuval Elovici, Director, Deutsche Telekom Laboratories at BGU 32

From Childhood to Maturity

Ms. Carmela Avner, The Government CIO 37

Second Session:

Cyber Crime

Crime, Warfare and the Psychology of Hackers

Mr. Misha Glenny, Writer and broadcaster, Author of “DarkMarket: Cyberthieves, Cybercops and You” 41

Managing Advanced Security Threats Using Big Data Analytics

Mr. Ed Schwartz, VP and CISO, RSA, the Security Division of EMC 47

Hacktivisim Comes of Age

Mr. Avi Chesla, CTO, Radware 52

The Dark Alleys of the Virtual World

Mr. Menny Barzilay, Head of IT Audit, Bank Hapoalim 56

Catching the Bad Guys - Lurking in the Hidden Cyberspace

Mr. Guy Mizrahi, CEO, Cyberia 59

Third Session:**Technological Aspects of Cyber Security**Cyber Security Lessons from Fighting Piracy in Pay-TV

Dr. Abe Peled, Executive Chairman, NDS Group Ltd 61

X-Force Trend Report 2011

Mr. Martin Borrett, Director of the IBM Institute for Advanced Security Europe 65

Trust No One - Information Security in a Hostile Environment

Dr. Eran Tromer, Blavatnik School of Computer Science, Tel Aviv University 69

Qassams and Cyber...

Mr. Michael Arov, Head of Information Security, R&D Section, RAFAEL, Advanced Defence Systems 74

The Need for Multi-Layer Cyber Intelligence

Mr. Mark Gazit, General Manager, NICE Intelligence Solutions, NICE Systems 77

Fourth Session:**Threats and Challenges in the Cyber Dimension**New and Renewed Threats in the Mobile World

Mr. Adi Sharabani, CEO Skycure Security 80

Constructive Ambiguity in Cyberspace: The Legal and Policy Challenges

Adv. Deborah Housen-Couriel, Yuval Ne'eman Workshop for Science, Technology and Security 83

The Cyber Threats on Developing National Defense Systems

Mr. Doron Rotem, Director, Crisis & Emergency Solutions, Israel Aerospace Industries 87

The Threats of the Age of Cyber-Warfare

Mr. Eugene Kaspersky, Chairman & CEO Kaspersky Lab . 90

Closing SessionRabbi Prof. Daniel Hershkowitz,
Israel's Minister of Science and Technology 96PM Benjamin Netanyahu,
Prime Minister of the State of Israel 97

Yuval Ne’eman Workshop and the National Cyber Bureau’s 3rd Annual International Cyber Security Conference – Creating Cyber Ecosystems – 2013:

| | |
|------------------------|-----|
| Conference Agenda..... | 100 |
|------------------------|-----|

Opening Session - Policy Makers

| | |
|---|-----|
| Prof. Maj. Gen. (Res.) Isaac Ben Israel, Head of the Yuval Ne’eman Workshop for Science, Technology and Security, Tel-Aviv University | 102 |
| Prof. Joseph Klaffer, President of Tel-Aviv University | 102 |
| Dr. Eviatar Matania, Head of the National Cyber Bureau, Prime Minister’s Office | 104 |
| Mr. Avi Hasson, Israel’s Chief Scientist | 107 |
| His Excellency Shimon Peres, President of the State of Israel | 108 |

First Session:

Cyber Readiness and Technology

Cyber Readiness: Is Any Nation Prepared?

| | |
|---|-----|
| Ms. Melissa Hathaway, President, Hathaway Global Strategies, LLC, Former Senior Director for Cyberspace at the National Security Council, USA | 112 |
|---|-----|

Intelligence-Driven Security: A New Model using Big Data

| | |
|---|-----|
| Mr. Art Coviello, Executive Vice President, EMC, Executive Chairman, RSA | 119 |
|---|-----|

Building Cyber Warriors

| | |
|---|-----|
| Mr. Paul de Souza, Founder & President, Cyber Security Forum Initiative (CSFI) | 125 |
|---|-----|

Leveraging SDN for Network Visibility, Security and Threat Response

| | |
|---|-----|
| Mr. Robert Shaw, CEO and President, Net Optics, Inc. | 127 |
|---|-----|

Wifigate - How Carriers Expose Us to Wifi Attacks

| | |
|--|-----|
| Mr. Adi Sharabani, CEO, Skycure Security | 131 |
|--|-----|

Second Session: Cyber War & Peace

Cyber War, Cyber Peace

| | |
|---|-----|
| Mr. Richard A. Clarke, President, Good Harbor Security Risk Management, Former Special Advisor for Cyber Security to the President of the USA | 135 |
|---|-----|

The Attribution Problem - A Fresh View

| | |
|--|--|
| Dr. Thomas Rid, Reader in War Studies, | |
|--|--|

| | |
|--|-----|
| King's College London | 141 |
| <u>Building an Effective National Cyber Defense – Capabilities, Strategies, Policies</u> | |
| Mr. Ilias Chantzou, Senior Director, Symantec Government Affairs-EMEA and APJ | 146 |

System Approach to Cyber Research

| | |
|---|-----|
| Mr. Doron Rotem, Director, Crisis & Emergency Management Solutions, MLM Division, Systems Missiles & Space Group, Israel Aerospace Industries Ltd. | 152 |
|---|-----|

Cyber Kill Chain™: Applying Intelligence to Defeat

Cyber Threats

| | |
|--|-----|
| Mr. Eric M. Hutchins, Fellow and the Chief Intelligence Analyst, Lockheed Martin (LM-CIRT) | 154 |
|--|-----|

Third Session:

Cyber Technology: The Next Generation

Singapore's Approach to Cyber Security

| | |
|---|-----|
| Lim Chuan Poh, Chairman, National Infocomm Security Committee(NISC) and Chairman, Agency for Science, Technology and Research (A*STAR), Singapore | 159 |
|---|-----|

Panel Discussion:

| | |
|--|-----|
| Mr. Eli Yitzhaki, Strategic & Business Development Leader, ELTA SIGINT EW & Communication Division | 165 |
| Mr. Avi Chesla, Chief Technology Officer, Radware | 167 |
| Mr. Tal Mozes, Hacktics Leader, Advisory Services, Ernst & Young | 169 |
| BG (Ret.) Yair Cohen, Head of Cyber Security, Elbit Systems | 171 |
| Mr. Andrey Dulkan, Director of Cyber Innovation, Cyber-Ark | 173 |

Fourth Session:

Hacking the Human Brain

Brainihack: How neuroscience can inform hacking and vice-versa

| | |
|---|-----|
| Dr. Moran Cerf, Neuroscientist, UCLA and NYU and ex-security expert | 180 |
|---|-----|

Towards HOMO SAPIENS 2.0

| | |
|--|-----|
| Mr. Yanki Margalit, Social entrepreneur, Chairman Spacell, Partner Innodo Ventures | 185 |
|--|-----|

The Bare Minimum: Emulating the Brain in a Computer

Dr. Roey Tzezana, Unit for Technology & Society Foresight at Tel Aviv University 188

Closing Session:**Cyberspace - The Final Frontier?**Cyber Inferno: 7 Circles

Mr. Eugene Kaspersky, Chairman & CEO Kaspersky Lab . 188

Ms. Keren Elazari, Introduction of the Yuval Ne'eman workshop's Senior Executive Forum Work Groups 191

The Applicability of International Law in Cyberspace - From If to How?

Prof. Catherine B. Lotrionte, Director, Institute for Law, Science & Global Security, Georgetown University 193

Terror Pornography, Gateway Websites, Drive-Thru Radicalization and Jihadi Cyber Weapons

Dr. James Van de Velde, Lecturer, Center for Advanced Governmental Studies, Johns Hopkins University; Associate, Booz Allen Hamilton 198

Appendix: Yuval Ne'eman Workshop for Science, Technology and Security - Researchers' Articles 202Critical Infrastructure Protection (CIP) against Cyber Threats: The International Cooperation Imperative

Lior Tabansky, Researcher, the Yuval Ne'eman Workshop for Science, Technology and Security. 203

A Multi-Faceted Strategy for Cyber Standardization

Deborah Housen-Couriel, Adv. and Admit Ivgi, Adv., Researchers, the Yuval Ne'eman Workshop for Science, Technology and Security 208

Participants' Biographies 213**Conferences' Sponsorships and Associations 229**

September 2014
Tel Aviv, Israel

Dear Friends and Colleagues,

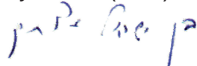
Around the globe, we live in the midst of significant technological and social changes driven by cyber technology. Research, innovation, entrepreneurship and sound policy are of crucial importance in times of such rapid transition. In line with the mission of the Yuval Ne'eman Workshop for Science, Technology and Security, we aim to promote and deepen both fact-based research and public dialogue which bolster and advance cybersecurity concerns.

The Ne'eman Workshop has established itself as Israel's focal point of interdisciplinary academic cybersecurity research and policy initiatives, as well as related activities and gatherings among experts at the highest levels on an ongoing basis. One outstanding example is the Workshop's advancement of public-private partnerships by holding a senior executive forum with the participation of defence officials, politicians, business leaders and scholars from leading Israeli and international entities. We also warmly welcome international cooperation, which has in recent years given our research and policy activities global exposure and recognition, and has also helped to sustain the Workshop's growth.

The Annual Cyber Security International Conferences at Tel Aviv University have showcased our work since 2011. It's my hope that the research and policy presentations included in the following Proceedings will interest you and deepen your understanding of key issues. From the presentations you'll find here of Israel's President and Prime Minister, government ministers, key government actors, and leading businesses and academics from Israel and around the globe, those of us who have participated in the Conferences have benefited from cutting-edge insights.

May the materials included here indeed contribute to deeper understanding, and to a more prosperous and more secure future for Israel and for the world.

Prof. Maj.-Gen. (Ret.) Isaac Ben-Israel



Head of Yuval Ne'eman Workshop for Science, Technology and Security

Dear Colleagues,

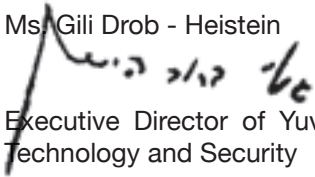
Since that first Conference we have come a long way in deepening the focus on Israel's cybersecurity capabilities and providing an open platform for global interest in them and increasing relevance to those concerned with the issues of cybersecurity, both in Israel and globally.

The high level of speakers and presenters has been a hallmark of the Conference from its inception, and we are pleased to note that the number of participants increases with every passing year. Participants (and speakers) come to learn, to exchange ideas, to get to know the Israeli cyber eco-system firsthand, and to make new professional contacts.

The following Proceedings of the past two Conferences of 2012 and 2013 will, we hope, be of interest as more than a record of the presentations made. It represents the cumulative work of many: of the presenters themselves, of course; and also of the dedicated researchers, fellows and professionals at the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University, under the leadership of Professor Isaac Ben Israel. In the next era of development of Tel Aviv University's leadership through its interdisciplinary academic approach to cybersecurity studies, future conferences will, we are confident, reflect its growing influence.

We welcome your comments on these Proceedings, and wish you an enjoyable reading.

Ms. Gili Drob - Heistein



Executive Director of Yuval Ne'eman Workshop for Science,
Technology and Security

**Yuval Ne`eman Workshop`s
2nd Annual International
Conference on:
Cyber Security – 2012**



Yuval Neeman Workshop for
Science, Technology
and Security
Tel Aviv University

You are cordially invited to attend Yuval Ne'eman
Workshop's Annual International Conference on:

Cyber Security

Wednesday, 6 June 2012, 07:30-17:45,
Smolarz Auditorium, Tel-Aviv University

Program:

07:30 - 09:00 **Registration and security check**

09:00 - 10:00 **Opening Session**

Greetings

Prof. Joseph Klafter, President of Tel Aviv University

Chair: Prof. Maj. Gen. (Res.) Isaac Ben Israel, Head of Yuval Ne'eman Workshop for Science, Technology and Security

Keynote Speakers:

Mr. Ehud Barak, Israel's Minister of Defense

Dr. Evyatar Matanya, Head of the National Cyber Bureau, Prime Minister's Office

10:00 - 11:15 **First Session: From Information Security to Cyber Security**

Chair: **Prof. Uzi Arad**, Former National Security Advisor to the PM and Head of the NSC

Uncovering Invisible Threats

Mr. Bob Shaw, President and CEO, Net Optics

Cyber Trends, Futures, and Road Map To Enhanced Security

Mr. Curt Aubley, VP/CTO Cyber Security & NexGen Innovation, Lockheed Martin

Social Networks Security

Prof. Yuval Elovici, Director, Deutsche Telekom Laboratories at BGU

From Childhood to Maturity

Ms. Carmela Avner, The Government CIO

11:15 - 11:45 **Recess**

11:45 - 13:15 **Second Session: Cyber Crime**

Chair: **Ms. Michal Blumenstyk-Braverman**, GM of Global Solutions and RSA Israel GM

Keynote Speaker:

Crime, Warfare and the Psychology of Hackers

Mr. Misha Glenny, Writer and broadcaster, Author of "DarkMarket: Cyberthieves, Cybercops and You"

Managing Advanced Security Threats Using Big Data Analytics

Mr. Ed Schwartz, VP and CISO, RSA, the Security Division of EMC

Hacktivisim Comes of Age

Mr. Avi Chesla, CTO, Radware

The Dark Alleys of the Virtual World

Mr. Menny Barzilay, Head of IT Audit, Bank Hapoalim

13:15 - 14:00 **Lunch Recess**

14:00 - 15:30 **Third Session: Technological Aspects of Cyber Security**

Chair: **Prof. Dov Te'eni**, Academic Director, Orange Institute for Internet Studies, Tel Aviv University and President of the Association for Information Systems

Keynote Speaker:

Cyber Security Lessons from Fighting Piracy in Pay-TV

Dr. Abe Peled, Executive Chairman, NDS Group Ltd

X-Force Trend Report 2011

Mr. Martin Borrett, Director of the IBM Institute for Advanced Security Europe

Trust No One - Information Security in a Hostile Environment

Dr. Eran Tromer, Blavatnik School of Computer Science, Tel Aviv University

Qassams and Cyber...

Mr. Michael Arov, Head of Information Security, R&D Section, RAFAEL, Advanced Defence Systems

The Need for Multi-Layer Cyber Intelligence

Mr. Mark Gazit, General Manager, NICE Intelligence Solutions, NICE Systems

15:30 - 16:45 **Fourth Session: Threats and Challenges in the Cyber Dimension**

Chair: **Dr. Nimrod Kozlovski**, Recanati Business School, Tel Aviv University; Chairman Altal Security

New and Renewed Threats in the Mobile World

Mr. Adi Sharabani, CEO Skycure Security

Constructive Ambiguity in Cyberspace: The Legal and Policy Challenges

Adv. Deborah Housen-Couriel, Yuval Ne'eman Workshop for Science, Technology and Security

The Cyber Threats on Developing National Defense Systems

Mr. Doron Rotem, Director, Crisis & Emergency Solutions, Israel Aerospace Industries

Keynote Speaker:

The Threats of the Age of Cyber-Warfare

Mr. Eugene Kaspersky, Chairman & CEO Kaspersky Lab

16:45 - 17:00 **Recess**

17:00 - 17:45 **Closing Session**

Chair: **Dr. Giora Yaron**, Chairman of the Executive Council of Tel Aviv University; Chairman of Ramot

Rabbi Prof. Daniel Hershkowitz, Israel's Minister of Science and Technology

Keynote Speaker:

PM Benjamin Netanyahu, Prime Minister of the State of Israel

Opening Session

Prof. Maj. Gen. (Res.) Isaac Ben Israel, Head of Yuval Ne'eman Workshop for Science, Technology and Security

Good morning Mr. Minister of Defense, President of Tel-Aviv University and distinguished guests. I am very glad to open the conference of Yuval Ne'eman Workshop for Science, Technology and Security, which in the ten years of its existence has held over 70 conferences. We have become aware that the cyber domain had entered the public awareness in the last couple of years, but certain circles had become aware of it some twenty years ago. When the Minister of Defense, Ehud Barak, served as the Chief of Staff, cyber activity started as part of the closed activity of the national security establishment. In the last couple of years we have come a long way, including the founding of a National Bureau within the Prime Minister's Office.

In my opinion, Tel-Aviv University will be the first in the world to open in the next academic year a course of studies which will be a combination of Computer Science Studies and Engineering in which students will be able to study for an undergraduate Cyber-Security degree

Mr. Ehud Barak, the Minister of Defense, will open this session because of two reasons: First, one can't deal with the cyber domain without talking about its security roots. At present we mark thirty years of the first Lebanon War and 45 years for the Six Days War [67 War]. Maybe one day historians will regard these wars as last of their kind. Future wars will be remarkably

different. Second, Minister of Defense is suitable to speak since it was in his tenure as the IDF Chief of Staff that the defense system began addressing this domain.

Prof. Joseph Klafter, President of Tel-Aviv University

Even if we don't hear "bang" sounds around us, that doesn't mean that there is no real war ongoing. If the newspaper reports are true, we are at present in the midst of the first cyber war in history: code-based battles with worms, viruses and Trojan horses have become an arsenal for all intents and purposes.

The world of science and technology and the realm of war have been intertwined in an increasingly growing intensity all along; be it the prehistoric blacksmith making arrow heads and spears or be it Edward Teller, "the father of the hydrogen bomb". Those responsible for conducting wars present new demands to scientists and engineers for tools and power, whereas the tools developers present growing and novel capabilities and possibilities that surprise those who need them. The cyber warfare is a milestone - the first of its kind in the history of war where the technology people are trying to strike the enemy's infrastructure and his ability to function and not necessarily at his physical existence. The cyber warfare is not only a matter of government versus government; the growing dependence of the economical system on technological infrastructure makes the entire societal-economic system vulnerable. According to the known data in the market, every year thousands of new IT security breaches are discovered. Under this reality the civil security market is flourishing and its value is estimated at 100 billion dollars. It is safe to assume that the knowledge accumulated in the security industry trickled into the civilian industries. This is what will happen in the cyber world as well.

Now, Cyber Warfare, like economics, places in the centre of balance of power the quality of the human capital. This capital is created and recruited in the academy's hallways and its lectures' halls. As it moves the gears of startup companies and makes the economy grow, it becomes the country's real power reservoir in the cyber era. Tel-Aviv University holds a focal place in the cyber warfare debate. The discussion here encompasses all of the aspects: from the technological aspect, through algorithm to the impact of the cyber era on philosophy and security policy.

Therefore, today, especially in the domain of cyber warfare, the higher education budget should be viewed as an integral part of the security budget.

Mr. Ehud Barak, Minister of Defense

I am very glad to be here with you at this important conference which addresses a very important issue and that its home-base is Yuval Ne'eman Workshop for Science, Technology and Security. I had the pleasure of knowing Yuval, and for me even to this day he is an exceptional figure in the Israeli experience. Yuval was a multi-disciplinary genius and a ground-breaking in his domain. Just as the cyber domain is new and virginal and entails creative thinking outside the box. Yuval's domain was Particle Physics and in his late thirties he had outstanding scientific achievements together with other research's partners, partners who won Nobel Prizes for outstanding contribution. Yuval's personality can serve as a source for inspiration for all those young people working in the cyber domain.

In the defense system at the national level we are taking the cyber domain very seriously and we in all earnestness intend to put Israel at the world's forefront in several domains: cyber as security system, immediate national preparedness, alignment and building solid infrastructures in both the security and civil sectors of the state of Israel. We are working in this domain due to the government's decision to form "The National Cyber Bureau". Dr. Eviatar Matania heads it and Isaac Ben Israel is the leader in this rapidly growing domain.

The communication and computer domain developed greatly and changed enormously in the last two decades. Reality surpassed all imagination. Even those of us who grew up into scientific or technological background could not foresee the scope and speed of those developments. On one hand, the technology and communication created outstanding political, national, operational, commercial and economical capabilities; on the other hand, the complexities of all the systems naturally created vulnerabilities. A fifth dimension was added to the national security equation - the cyber dimension. The ability of a country to defend itself and its vital interests, national infrastructures included, include today the ability to withstand the cyber threat.

The cyber roots are in the first computers. Once there are abilities, there are also abilities to harm and disrupt. The significant change we are experiencing of this unfolding revolution - is also the reason for this conference. And the real change is in the ability to harm once the systems become more complex and sophisticated. In military aspect, one can compare the entrance of the cyber to the great revolution in war fighting: the

arrival of the tank some hundred years ago and of the airplane some seventy years ago. These developments created a much bigger change than could have been imagined. The futuristic destruction potential embodied in the cyber arena is similar to the destruction potential of the more sophisticated systems, even though destruction is not directly causing loss of human lives.

In the civil sector, the critical infrastructures of every country are vulnerable. Cyberspace in itself is a vital infrastructure, but so are the water, gas, electricity and communication infrastructures; intellectual property; the financial system and even private, intimate information. Nowadays, there are millions of cyber attacks and a significant number of these attacks have a high harm potential. The systems they are directed to and the overall damages of these attacks is estimated in billions of dollars.

In the military and operational sector we are witnessing the growth of the asymmetrical threat: terror, assimilation within the population, rockets and ground to ground missiles that bypass aerial superiority. This trend of a-symmetrical development the cyber brings to a new height: a single able hacker can cause huge damage to great economical systems or to national systems; and yet we have not reached the peak yet.

Operating in the cyber space greatly enhances the power of individuals sometimes working from a small room to inflict harm and to operate. The free world is facing a threat mainly from terror organizations, crime organizations and rogue states. Today, the means required for adequate response to the cyber threat are yet to be developed- not on national level of neither of the countries and certainly nothing regarding global international cooperation. This fact raises the level of threat since the implications of action or hit on one society can influence other societies. The cyber activist attacks do not always care about national borders or borders in general. A cyber attack on the database of one big stock-exchange can cause a clearing of transactions that have already been carried out. I assume that alongside these abilities and phenomena, a wider response will evolve – in the level of the sole organization and in co-operations between states and international organizations. However, today, we are far from achieving it. I will introduce three components that characterize this battle:

- The attribution problem: It's hard to simply determine if it's a malfunction or external attack. And when professionals on both sides are involved, the matters get more complicated.

In cases in which the attack was identified, identification of the attacker in the world of servers is not simple. The deterrence element which in the past was one of the obstacles to prevent further escalation wore out considerably. The capability of direct reaction is also problematic. In addition, technically, we don't know what we have to do; and it finds its expression also in the legal aspect where the problems stem from absence of rules and legal norms of how to deal with this field.

- Blurring of the boundaries that exist at present between peaceful times and war. In traditional wars it was clear when you were at war and when not. In the cyber field, combat expands to times in which there is no overt or declared war, and yet there is an activity from more than one side.

- The implications of cyber attacks on the security sector and the civil sector and the interdependency between them. Our systems, including defense, rely on the national civil infrastructure that is interconnected with the Transport, Energy, Economy and Communication systems and to the national financial systems further more than how it used to be in the past. Therefore our ability to confront the cyber threat is defined by the weakest link and not the strongest one.

What can be done in order to provide a solution? To begin with, in order to be able to cope we ought to get organized at the individual, the organizational and the state level. A comprehensive integrative concept is required. Later on, when something is identified we need to check it, consult, analyze and try to solve it. Nowadays we are unable to keep up with the pace and volume, therefore a transition to a pro-active approach in which passive gathering of intelligence- a kind of autonomic continuous staring at very wide domains, is required- in order to identify anomalies. In addition, we ought to move to a transition from a specific limited reaction into a wide systemic reaction, almost in real time. The analysis can't be an analysis of the single action and comparing it, but the use of wider data-bases and other approaches is required. All these things ought to change both from a conceptual point of view and operative one. Our aim in security, which is the more challenging domain, is to promote the right defensive behavior. All these challenges will require constant cooperation among the high-tech industries, the security sector and the academy- not only at the national level, but also at the international level.

To sum up, in an era where the entire virtual world becomes more tangible and real, cyber warfare will not be the problem of

one single country, but of us all. In the unique conditions of the State of Israel, we need to create a balance of deterrence and the ability to act effectively in the new world which is a world that its ability's limits rely more than anything on the human mind, on human abilities and excellence of infrastructures- Israel is blessed with an abundance of these all.

Dr. Eviatar Matania- Head of the National Cyber Bureau.

I'd like to concentrate on the main directions in which the National Cyber Bureau which I head deals with and will deal with in order to enhance the security of Israel in cyberspace.

Several aspects guide us at the Bureau. The first aspect is the absence of borders and what it means on the national level. Unlike in the past- when we classified threats by countries with which we share borders and more distant countries, now when we are talking about the cyber threat, the entire world is actually the front line. This absence of borders impacts another aspect at the national level: sovereignty is unclear, and the threat is not met by a buffer of the army or other security organizations. The cyber threats bypass all military power built to defend from various traditional threats, and reaches directly to the heart of the country. Therefore, one of the most important challenges is to alter the security arrangements, and connect them and the civil society.

Another aspect is the amplitude intensity of cyber threats: from what is called a "super tactic"- a really small threat that can harm a home computer to a strategic threat that can ruin critical state infrastructures.

The cyber threat is not just wartime or emergency time threat, but one that is always there. This threat has also wide-scale psychological aspects and many researches have shown that our ability to cope with threats increases as the threat is confined in time and place. The more we estimate the threat as present everywhere at all times, our psychological ability to cope diminishes.

The leaders, industry, academy and the defense system- all recognized these issues; hence they led to the establishment of the "National Cyber Initiative" two years ago led by Prof. Ben Israel. Last year, at the inaugural cyber conference, PM Benjamin Netanyahu adopted the team's recommendations. According

to the government's decision, all insights that were formed in the project were adopted and a National Cyber Bureau (INCB) was formed a few months ago reporting directly to the PM. The INCB is working to develop the Israeli cyber-defense industry, additionally the bureau oversees policy to protect and promote the necessary infrastructures to be able to cope with the threat properly.

The bureau has started its activity according to the government's decision and presented a full work-plan for 2012-2013 year along three main courses

- To design a national cyber-defense concept for the state of Israel, enhancing cyber-security in Israel throughout business and government sectors by promoting appropriate regulation
- To develop the cyber-security market by promoting standard qualification criteria so that there will be a regulated, real and strong market in Israel to support various organizations and
- To raise awareness and provide information to all sectors.

I'll provide some examples to actions we are already conducting: we have launched a joint pilot program with the Ministry of Energy and Water Resources to map all utility related companies and engage them to raise awareness and preparedness. The management will evaluate the risk and come up with a work plan to more efficiently protect the companies. we started the process with one of the companies in the water sector. We will deepen and spread this process in this sector and we will also turn to other sectors. For every sector we will prepare a set of regulations and instructions for all the companies to follow in order increase cyber security. We will set up a committee responsible for designing such regulation while preventing unnecessary burden suffocating innovation and business.

Yet, protection is not enough and a transition from protection to cyber security is coming. Security is not just building higher, stronger fences. We don't fight terror just with fences, but with a complex process of Intelligence and information sharing among various bodies. The second layer is therefore the forming of a national defense plan and in the near future in its center will be the national cyber situation room. This will address intelligence sharing among the various organizations, especially the connection between the defense and the civil

systems. Here lies one of the biggest challenges, since before the cyber challenge such a close connection was not needed. The national situation room will enable comprehensive national monitoring and situational awareness. When someone attacks somewhere, we'll be able to know the implications on another place and defend it accordingly. Once the situation room is operative, we'll start the transition from protection to cyber security. Dealing with forming a national defense concept we focus on promoting Israel's infrastructures. The first and most important one is the technological infrastructure which is an essential, crucial part of our capability to face the threat. And the INCB job is to allow the academic and the industrial sectors to progress together. We have created together with the Ministry of Science a research grant fund of 50 million Shekel in total, for research and scholarships for Master and Doctorate candidates. It is actually the academy that conducts research that will make us excel and lead in the world in cyber-security. In my view, increasing the number of excellent MA and PhD holders in the workforce will help to successfully introduce training and undergraduate courses, advance research to be implemented in the industry and develop the workforce. However, alongside investing in academic infrastructure, we ought to promote the industry in Israel. This is the government's task to find the required tools to leverage the country's potential. The example I use is the very establishment of the "Yozma" plan in 1993 by the government- the first venture capital fund, which actually spawned the thriving venture capital market in Israel and thus promoted the high-tech industry. The government's initial investment of 100 million dollar yielded dozens billion dollars. We just held a meeting with all R&D industries in order to present all possible directions: starting from financing greenhouses, a cyber oriented R&D fund, building "excellence centers" and other ideas. I believe that as a result of this and other meetings with the industry we will be able to introduce relevant measures that will be operative in 2013. This includes designated plans of funding research and national level projects and tools of the sort of funds and greenhouses that will let this industry flourish. The third dimension, apart from academic and industrial infrastructures is the national laboratories. In this field we have started to operate together with the academy and others in order to understand what are the national infrastructures that Israel ought to have in order to promote all other infrastructures- both academic and industrial alike: infrastructures like

forensic knowledge, hardware and other. Later on we will see to establishing the relevant laboratories together with the academy. Additional infrastructure that is one of the most important infrastructures existing in the cyber field is the human infrastructure. Developing elite human resources, which are the very engine the high-tech industry, is the task of both the academy and industry. Among other things, we are cooperating with the Ministry of Education to better direct the education system so there will be more students trained for these fields, within one to two years these resources will increase.

A lone country cannot deal effectively with the cyber threat. If we want to move forward we ought to cooperate with other countries in the world, be part of the alliances made in this field, and be part of the civilized world that fights cybercrime, on which terror and political threats ride. We are promoting together with the Ministry of Foreign Affairs, Ministry of Justice and all other relevant elements a proper position for Israel in the international community. I believe that joining the world in the subject of standardization, alliances, and treaties with the relevant countries will be a complimentary layer to the two layers I've described.

Our vision towards which we march is promoting and developing of defense systems for the state of Israel in the cyber world side by side to developing and promoting the infrastructures in order to be the leading country in this domain. I believe that a lot of what we understand and do today will change with the technology that grows at crazy rate. Hence, a significant part of what we are doing is building infrastructures and robust tools, to use even when the insights will change. I believe that real partnership with the entirety of the elements in the market and the various sectors in this field could place Israel in the right place. In my view it is the role of the Bureau as a leading body together with all other agencies.

01

First Session: from Information Security to Cyber Security

Uncovering Invisible Threats

Mr. Robert Shaw | President and CEO, Net Optics

Net Optics works with a broad set of costumers around the globe. In the world of telecom providers, it is the AT&T, the Vodaphones, the Vevo's in Latin America, Vympelcom in Russia. Net Optics also works with large financial networks such as American Express, the New York Stock Exchange, the Brazilian Stock Exchange, Credit Swiss, Morgan Stanley, and Barclay's. Data and networks are critical for all these organizations. Additionally, Net Optics works with all the government agencies to ensure that they are architecting visibility into their networks. Net Optics will announce in Q3 the opening of an R&D center in Israel, which could also be considered a center of excellence. Net Optics was founded and is chaired by an Israeli, Eldad Matityahu. Since its founding in 1996, Net Optics has grown 64 quarters in a row, and it has done so without any VC funding. Every 15 minutes, 10,000 records and costumer data are compromised around the world. 95% of those 10,000 records, will be stolen, hacked and taken, undetected by the organization from which they are taken. An organization, be it a government agency, a telecommunications company or a financial organization, will have data extracted from its network and the network itself will not even know that is the case.

This situation can be rectified.

There are many great tools in the market, and as a result, companies or agencies are sometimes inclined to think that the

solution is relatively simple. With the appropriate security tool, an organization should be able to put it into its network, turn it on, and let it work. However, it is a little more complicated than that for a number of reasons. Leaders of major organizations, be it government agencies, telecommunications companies or financial organizations, are attempting to get visibility into the network. The missing ingredient is the question how does one have insight; how does one have visibility; how can one be proactive by knowing what is going on in the network. There are several challenges. Network design is complicated; data centers, remote branches, everything is now moving to the cloud in virtualization, creating, in a sense, stacks. There is a multitude of people in each organization responsible for security, compliance, applications and database. Usually, the people responsible for these fields agree on the need for visibility in the core part of the network. However, transferring this solution of visibility to cloud often involves a different group or individuals. A group of people that are actually in charge of visibility and making sure it is architected into the network across all the disciplines is required, from the remote branches, through the data centers - the core part of the network - and to the cloud and virtualization. This type of organization provides the ability to be proactive and to anticipate and move away from being reactionary.

The networks that are most likely to be attacked are those running at faster speeds. Networks are moving from gigabit-per-second to 10 Gig, soon to be 40 Gig; and in many cases, telecommunication companies have already rolled out 80 or 100-Gigabit network speeds. A network that is running at 40 gigabits or 80 gigabits requires security tools. The best security tool in the market today, when loaded up with all the rules, will run at 10 Gig, and some are getting very close to running at 20 Gig. With 40-, 80- and 100-Gig networks requiring tools, a balance develops. The network must be secured for customers, but performance is also important. Balancing between these two needs is an important choice for organizations.

A set of tools becoming available is called 'access switches'. This is different than a switch and router, but it is between those two. It allows taking data that is running at 40 and 80 Gig and collecting all of that data in various parts of the network, balancing and sending it across tools that cannot run at the network speed. This enables utilizing three or four tools together to view traffic in high-speed networks. This creates visibility while at the same

time allowing access and performing security tasks in real time. This particular solution, bundled with one of the leading security companies in the world, received the Best of Show solution award in Interop trade show in May 2012. This is the only solution in the world right now that is a bundle. Installation of this solution enables looking at 80 Gigabits of traffic in real time, examining every packet and determining if there is a risk to the network. It is a source of excitement that Net Optics has created the device. It is OEM'ed. It has the other company's name on it, but it is manufactured at Net Optics facility in California and shipped all around the world. It is a game-changing technology.

There is another aspect that requires consideration. The industry has crossed an important point. As of the end of last year, there were more virtual servers installed in the network than physical servers. Cloud and virtualization are here to stay. One of the biggest risks that an organization must examine is how it could achieve visibility and see what is happening as traffic moves across the inner Virtual Machine traffic. As traffic moves from virtual machine to virtual machine, organizations are blind. This can be seen in the first virtual server and the last one, but as it moves through different geographic locations and from server to server, organizations are blind to it. To solve this problem, Net Optics has invented a piece of software that actually sits at the kernel level. The customer can pick whatever solution it wants, KVM, Hyper-V, VSX - and will also have the ability to look at all of the traffic in its cloud and virtualized world and the ability to pull that virtualized traffic and view it using physical tools. This creates visibility not only across the virtual world, but also in data centers and in remote branches, which is critical for success. The key lies in making sure that there are no blind spots. An architecture that allows complete visibility wherever needed at any given time is created, and it will enable taking tools already invested in to get an ROI. These can be scaled without dramatically changing the investment strategy, because tools already invested in can be used to look at parts of the network that were previously invisible.

Today, 94 to 95 percent of all security breaches are reported by someone outside the attacked organization. For General Electric CIO, particularly in relation to its government-agency customers, one of the most critical points regarding visibility is making sure they can be very proactive and be able to anticipate what is needed to do at any given moment. If it is necessary to give an incident report, they have the information in front of them

and they can be very proactive.

As a final thought on the overall architecture of a network - every network is going to be different. A main issue becomes what switches and routers are used. One critical goal is ensuring visibility across the network. A whole series of products that are shipped all over the world has been architected by Net Optics. These products allow taking data and channeling it to whatever tools desired. Blind spots can simply not be afforded and there is technology available that can help eliminate these blind spots. A group of people in every organization should always be seeking to increase visibility and access to data, especially as networks are built and expanded.

As Net Optics continues to grow, the VP of technology, Sharon Vesser, and VP of engineering, Shlomo Garfinkel, are going to help the company to build and launch the new R&D center of excellence.

Cyber Trends, Futures, and Road Map To Enhanced Security

Mr. Curt Aubley | VP/CTO Cyber Security & NexGen Innovation,
Lockheed Martin

Lockheed Martin Information Systems and Global Solutions is a 10-billion-dollar division within Lockheed Martin. It is the top IT provider for the US government and it runs a full life cycle for security from advanced R&D through security operation and security intelligence centers with approximately 2,300 customers around the world. We will cover some of the bigger trends in the market, then discuss a little bit about two different frameworks that are used for both the analysis and road map to improve security posture. When discussing security, the first thing to think about is the goal. What are you trying to achieve: national security, safe infrastructure, safe personal identity? Some technology companies say they are all about cloud and others are about security. Lockheed Martin is about customer success - be it business objectives or mission objectives. Though cyber security involves a great deal of technical detail, at the end of the day, the product being provided is the ability to fight through an attack. Power systems and banking systems must not go offline. Attacks are not supposed to prevent a company from achieving its objectives. This is the bigger picture trend. It is not really about cyber security. There is usually a separation between networks and this is part of a mega-trend taking place. In some of these trends - smartphone, social networks, new consumer expectation, and commodification - Lockheed Martin sees a converged life coming. Experts are talking about 80-Gig per second data rates or more. Advances and changes are not happening at stepping stone speed, but rather exponentially moving across the board. This creates a lot of opportunities; a

level of personal awareness that people have never had before; and great collaboration. People tell Facebook every little thing they do, from eating a pizza or going the beach. This creates opportunities to collaborate, but also creates the possibility of new attack surfaces for adversaries to take advantage in order to meet their objectives. These adversaries are many.

Lockheed Martin has categorized the entire security world into four little buckets. The first one: physical security and supply chain. Without physical security and some level of insurance and trust of a supply chain, no enterprise is secure. The next bucket is called 'the 80% known threats'. These are threats that are not easy to manage, but using commercial off-the-shelf technologies and following the best practices such as those of the SANS Institute will probably stop 80% of the threats. Beside the 80% known threats are the 20% advanced threats or unknown threats. This involves exposure to hundreds of thousands of new pieces of malware no one has ever seen before. Stuxnet, Flame, and others were made by well-funded, well-organized groups that test all their tools and malware against all the tools that can be bought off the shelf. Then, there are unique capabilities that different civil, defense or intelligence groups might need. In the world of cyber threats, there are software development tools that make it easier to develop software. There are a host of cyber security tools that are point and click. Some tools, like 'Zeus' malware family, can be purchased on eBay and come with a maintenance plan.

Some of the common threats seen today include e-mail spoofing. This was popular in 2006, but most people knew it was not wise to purchase an item from Nigeria for 10,000 dollars with the promise of receiving one million dollars. Today, cyber attackers look at supply chains. A smaller company with which a large company works on a daily basis can be compromised. An individual can get spoofed without knowing their identity has been taken. Then, the attacker can attempt to attack the larger company with greater ease, appearing to be a trusted source. Lateral movement, jumping across networks now through social means: fake sites were once relatively common. Today, attackers turn straight to infecting the legitimate sites. Two-factor authentication was a fairly good method - and it still is, but without the right methods, even two-factor authentication is being compromised.

What can be done in order to manage these risks and ensure resilient solutions? Lockheed Martin has created a framework to provide the defender with the ability to win. It is often said that a defender has to be right every time because the offence has the advantage. This is not necessarily true. End-user training can help prevent many types of cyber-attacks and exploitation methods. It is important to understand cyber adversaries better, because a defender who understands how an adversary works can put counter measures in place.

Lockheed Martin's 'Kill Chain' analysis provides the ability to deny, disrupt, degrade or deceive an adversary. If an attacker can be stopped in the reconnaissance phase - that is being very proactive. Network situation awareness is very important in case an attacker is able to deliver a new form of malware. The ability to detect such malware in a resilient or integrative fashion is still good, but it is not desirable to wait until the attacker is done creating a command and control channel to the outside world. It is preferable to find them as high on the chain as possible in order to enable proactive measures.

Many customers know information about their adversaries; recognize the trends; and face a very big challenge defending a rapidly changing environment in order to keep up in the business world. These customers want to know what measures they should take in order to improve their security posture. Step one: defend the enterprise. Step two: ensure business success. The foundation requires having the right people, the right processes and the right technologies in place.

In terms of defending an enterprise, there is a series of steps that help a customer; and this is used internally as well in order to improve the customer's ability to defend. It is important to have metrics - how well the company is doing. It is necessary to have the right people, trained appropriately. This is why there are school systems and universities, and collaboration becomes highly important. These collaborations should be organized in the most effective fashion. It is difficult to take someone immediately from school and put them directly into a cyber defensive situation. They need to learn the tradecraft. They may have learned quite a bit on their own, but Lockheed Martin can provide training for customers that allows them to advance this tradecraft and really understand the adversary and be able to defend the company. The supporting technology is important, but if a company does not have the items above it, technology is actually quite worthless.

There are many different levels of preparedness in cyber security. The first level is ad hoc and basically involves hoping for the best. This level is not recommended. Level two means becoming a spectator, having limited computer network defense collaboration. The defender starts listening to different vendors; it develops defense concepts and starts putting some of the pieces in place. Perhaps an alert occurs once in a while and a security incident is opened. Level three is when the company starts becoming a consumer of cyber intelligence and better understands the security awareness of the network. At this level, the company will have real metrics. Incident tracking and mapping can be integrated into the company's kill chain methodology. It becomes possible to look at campaigns. If something happens once, it's bad. Two things happening from the same actor is a little bit worse. If three, four or five things occur, then the company can recognize the same adversary attacking its network over time. Now the company is in the right direction, as it is possible to understand what the adversary might be doing. From here, the company can move to level four, which is becoming a producer of cyber intelligence. Becoming a producer of cyber intelligence means sharing it with the community.

Cyber security is a team sport. There is always a risk, because if the attacker knows that the defender is aware of the attacks, it might change its tools, techniques and procedures. Therefore, a defender must exist in an environment where there is trust in relationships and information is shared. This means looking at the 20% metrics. This requires fusing the intelligence to attain extensive situation awareness; training end-users; training engineers and administrators; and even training the executives to allocate more money for cyber defense.

The final leap is to level five, where a company becomes involved in cyber prediction and utilization of techniques such as open-source intelligence and attains the ability to help the community at large. The level at which a company chooses to operate is a decision for that individual company. Every environment is different. Lockheed Martin can provide a capability maturity guide to help a company move to any level or goal that it is trying to achieve.

Social Networks Security.

Prof. Yuval Elovici | Director, Deutsche Telecom Laboratories at BGU

I'll talk about Social Networks Security: a field which presently I'm trying to promote, especially the research, although I believe that soon enough it'll dive into product development. Today's information security solutions focus mainly on tangible things like communication networks, servers, endpoints and mobile devices. In the latter field a lot was done lately.

Nowadays we know that users spend a lot of time on social networks and it's clear that social networks constitute a large part of the cyber space. Although networks are less tangible than cellphones, social networks require protection as well. There are some unique threats to social networks and actually it's impossible to cope with them with the standard security means that were developed for other infrastructures like computers and servers.

Firstly, we have to be able to identify those unique social network threats; then unique solutions that can protect users on social networks need to be developed. There are three different levels of the implication of threats on social networks' users: level of national security, level of business security and level of the individual's security and privacy. I'll demonstrate how companies and individuals can be impacted from various threats lurking on the social networks.

I'll give some examples that will describe threats relevant to the first sector: national security. The first example: many people feel free to reveal information on social networks. There are cases when soldiers provide operational Intelligence to their friends in the social networks and it is well known that the

enemy is capable of creating and operating fake user profiles on social networks and thus able to collect military intelligence that we wouldn't want to fall into their hands. These things might be done innocently by soldiers sharing with their friends, but it might damage Israel's national security considerably.

The second example is a conversation in which the names of commanding officers and senior people in the security system are mentioned. People tend to reveal the names of senior people or their code names- usually innocently. A thorough analysis of the intelligence spread on social networks can allow the enemy to chart an organization within the defense system.

The third one is influencing groups via social networks. In recent years, scientific research was conducted in order to understand the diffusion mechanisms of opinions within social networks. The implications were that once we understood how opinions bubbled in the social networks, we could, with the right wiring, connect to certain people with hardly any effort, and influence the opinions of a large group of people.

What are the security implications of these threats? Actually, mainly at times of war the enemy will try to induce de-moralization by distributing misinformation at different places on social networks. Such a thing can be very harmful to national security. In the second field, threats in the business sector sometimes are referred to as "business opportunities". Social networks serve as platforms for industrial espionage. Often, innocent information a person tells his network friends might reveal a lot about the business operations of the company. For instance, when a mergers' director writes his friends that he is going to Finland (and now is the middle of winter) there is a big chance the reason he is going for is some business opportunity. And in this way a lot can be concluded about this director's company via the social networks.

It is important to say that it's relatively easy to locate those people on social networks like Facebook. For instance, from a research conducted on LinkedIn we learnt about organizational structures. On this social network people tend to declare in which organization they work and their position. We have learned that many people state their position in the organizational hierarchy. Many organizations are interested in hiding organizational changes they are making, but once the people working there update on LinkedIn their new position, outsiders can learn about the organizational changes carried out though keeping an eye on the social networks. After identifying a certain person according

to his position, it's possible to find him on Facebook and so learn about his life and the company he works at.

Another problem is the spreading of malicious rumors. It is possible to spread malicious disinformation about a product of a certain company and inflict tremendous damage to the company.

The last field of threats is threats on friends on social networks. The first example and actually the most problematic one deals with the very essence of the meaning of privacy. When a lawyer is asked what is the meaning of the term "privacy", he will define it as the ability of an individual to control the spreading of information about oneself. Hence, supposedly, social network is an excellent platform in which a person can tell about himself certain things he is willing to reveal in front of all the other people. The problem lies in the fact that once I link with other people on social networks, they know I'm their friend and can provide information about me but not necessarily only about me, also information about them. Through this much can be learnt about me. In Facebook for instance, in my profile there are a lot of things you can learn by analyzing the contents my friends told about themselves. So issues like hiding one's age or sexual preference are irrelevant on social networks, since this information can be deducted via my friends.

Second example: it can be proved that you know someone via social networks. This field is called "link prediction"- that means, the ability to prove an existence of a connection between two people on social networks. The main implications are in the world of intelligence. In this case, the implication on a social network user is that when a person states he is connected to a certain number of friends, it's possible, using techniques of link prediction to prove that he also knows another person, although he did not wish to let it be known. It can be deducted by analyzing the internet but then the user's privacy is invaded.

Third example- the problem of the "unwelcomed user": when malicious people start a fake profile and try to reach and contact us. For instance, a pedophile creates a fake profile and tries to connect to young girls. Once he gains their trust, he can sexually assault them.

One of the common things to all cyber-threats is that harm is done by fake identities. One of the things that can be done against it is to develop techniques to identify those fake identities. As of today at least six percent of Facebook profiles are fake. There

are two kinds of fake profiles: 1. When somebody pretends to be someone famous in the real world on which the perpetrator wants to rely on; 2. When someone creates a virtual, non-existent identity with various characteristics that entice people to come in contact.

In a research we have conducted, we tried to develop at least two different mechanisms that can remedy this. The first solution, "Social Privacy Protector", is aimed at recommending to us what friend we'd better "unfriend" since he is probably a fake figure. The second solution is called "Social Institution Detection" and it tries to identify a specific identity as fake.

One of the characteristics of a fake identity on social networks is that it has some anomaly. For instance, the profile is connected to many isolated communities and to a large number of disparate profiles. It's relatively easy to expose and declare it as a potentially fake figure. Another way is to use "Link Prediction" method, in which a potential connection between two identities is analyzed to estimate whether it's a reasonable one by checking the likelihood of each of its connections. If the majority of the connections are unlikely, then we may assume it's a fake trying to get mapped to specific locations on the net. There are many other directions for future research for ways of identifying fake identity on social networks. Any solution will provide only a partial answer that will be suitable only for part of the risks. I'll conclude by saying that the open issues in the field of social networks security are very big. First at the national level- when a country decides it wants to protect its citizens' social networks, it faces great difficulty on the operational stage, since not necessarily it has access to the particular social networks and not necessarily we'd like the state to be a kind of "big brother" that can {over} see everything on social networks. On the other hand, as I have said before, the social networks might prove to be a great risk to the state.

An additional problem is the one of information leakage via social networks. Companies face a severe problem of information leakage and it is one of the central issues in the area of information security; and the majority of the tools of coping with leakage of information are actually inside the organization. What an employee posts on Facebook is beyond the organization's access, hence the question remains how the organization can protect itself from the risk of leakage of information via social networks.

Tools that enable the protection within the internet and also

provide the benefit of linking to other friends on the internet ought to be provided to individual users. Many people are interested in getting to know others via social networks, hence it's hard to prevent someone from connecting on social networks to people he does not know. On the other hand, we ought to give him tools that will let him understand the risks embodied in his doing so. That is problematic especially with young users whose ego grows bigger the more friends they acquire.

From Childhood to Maturity

Mrs. Carmela Avner | the Government CIO

Lately I was appointed as the Government Chief Information Officer, which is a new position in the Israeli government. In my former position, I was the director of E-government. It's the first time the government has a comprehensive view of ICT in all government ministries. I called my presentation "From Childhood to Maturity" since when you look at organizations' communication and information security systems, they are in a process of growing.

E-government was the first organ the government established in 1986 in order to provide citizens and businesses easier accessibility to all technological services and to detailed information via internet. Likewise, it had to ensure the government is keeping in time with the services it provides. After being founded, it turned out that one of the principles or core activities of E-Government was information security. Nowadays, databases and interaction amongst them are protected, but lately the internet is rustling with activity and cyber warfare has become a reality. We cannot refer to information security as a war- something with a beginning and an end, but as an ongoing effort. Hence, information security for us is a way of life.

In this field we can't talk about an "isolated island" – a closed system of computers of government offices or private computers, or even a public computers' network. Nowadays the topic is broader. There are attacks against government offices whose origins can be identified, but there are also attacks that originate from locations we are not aware of.

The government can claim it needs to protect itself and not

provide these services to the public, citizens, community and businesses. On one hand it's our interest to be more open and use social networks, smart phones and other media; on the other hand we ought to be aware of the conflict of information security between the accessibility to information and securing our privacy, securing the privacy of the government organs and mainly securing the information and privacy of the citizens.

One of the goals of ICT bureau is to make sure we have the accessibility and availability to information and processes, both intra-government between government offices and their customers. At present there are more online services provided by the government than ever. Bills can be paid, information found and all sorts of activities can be performed over the internet. If this information is compromised, we may harm the citizens' welfare. Everything can be done in the old fashioned way, but in order to advance and improve citizens' welfare, it's preferable to advance e-Gov with ICT.

Accessibility and availability are our main concerns. Since our world has become more complex, every hit at any of the operational systems must be checked. Firstly, malfunctions need to be checked-whether they are malicious attacks or spontaneous "normal" malfunctions. One of our challenges is to verify whether the anomaly that exists in the operational system is normal or not.

What is the meaning of normal anomaly? Bill Gates systems that randomly freeze have become a part of the norm. In the past we were not used to such things and if occurred were considered as exceptions. Nowadays, DDoS- Distributed Denial of Service - has also become a routine matter. Such attacks exist and we have to see how to deal with them and recover from them quickly. A solution has to be found for distinguishing between initiated attacks of deliberately crashing down services and ongoing activities. The government has to be judged according to its capability of locating the problems- whether it's a problem of malfunction, a cyber-attack, a superficial event blocking access to a service we provide or an event that might cause damage like data's destruction, identity theft etc. In a case of a serious event that has penetrated our core system and manipulated the data, the problem still exists if we are too late in locating it. Firstly, rapid identification tools apart from defense tools must be developed. The sooner the malfunction or hit is located and identified, the faster recovery is possible. Secondly, we have to understand our recovery capability: what is required to restore a

system after a failure and how long it will take. These processes are far from simple.

In this aspect, the government is a very conservative bureaucracy. We must integrate the new tools, the new approach and the new threats to keep our assets and system up to date and protected. For that purpose, as part of the new ICT Bureau, I'd like to develop better integration of new technologies to assist the government response to various challenges.

I called my presentation "from Childhood to Maturity" since at adolescence, for the first time we are aware of ourselves and our actions. At this age we are probing into our own identity and asking questions like "who are we"? And in our case - do we, as an organ, only have to make the data accessible or do we have to protect it as well? Boundaries have to be set. The use of smart phones allows us to work for our company and at the same time to manage our private lives. It's hard to separate the worlds of work and leisure

The world today entails rapid reaction; hence baseline standards have to be defined. We have to check our boundaries, be they cultural or technological. Setting these boundaries without diminishing the value of cooperation and transparency is our responsibility, at the government CIO.

At adolescence we also begin to understand who and what we are, develop ourselves and start long term planning. In the aspect of cyber security – long term planning is a way of life. To promote road safety, rules, awareness and training are developed side by side to pressuring the market to produce cars with safer technology for public's protection, in order to protect ourselves. Similarly, we ought to plan ICT for the long run. We ought to plan them in advance while taking into consideration the new life style. There is a need for constant future planning since technology gets constantly more advanced. We ought to be prepared for confrontation with awareness and capability for rapid recovery to minimize the impact.

One of the government's goals in the cyber domain is the development of human capital, required for defense and long term planning of systems' infrastructures, and to partner together with the private and business sectors for defense purposes.

The government's ICT bureau is, in effect, a new authority or administrative unit with several responsibility areas including all-government ICT strategy. E-government has actually been the government's harbinger to make systems and data accessible. One of the goals of ICT bureau is to leverage it and enable better,

more secure, open government services to the public.

The bureau will also define the behavior, standards and policy for government's ministries, to verify that all services are functioning in unison. In the cyber fields ICT bureau is cooperating with the National Cyber Bureau that was established recently at the PM's Office, and likewise with other organs like the National Information Security Agency (NISA), the Israeli Law Information and Technology Authority [ILITA] which is part of the Ministry of Justice responsible for privacy regulation, and others.

One of ICT bureau important objectives is raising awareness, not only within government offices but with business sector. For instance, from the publicized attack of the so-called "Saudi Arabian hacker" we learnt that the public and small businesses were craved for reliable information. Consequently, as a joint initiative with the National Cyber Bureau, ILITA, and internet authority, public security and other agencies, "cyber.gov.il" portal will be launched to respond to public demands.

A public campaign to raise cyber security awareness, and safe behavior on the internet is planned.

To conclude, in the cyber field the ICT bureau goal is twofold: to provide Israeli citizens education on digital citizenship and, from the technological aspect- to maintain innovativeness in order to improve the security and resilience of government ICT systems.

02

Second session: cyber crime

Crime, Warfare and the Psychology of Hackers

Mr. Misha Glenny | Writer and broadcaster, Author of "DarkMarket: Cyberthieves, Cybercops and You"

To write a successful book about computer security that will be read by people other than geeks, what is needed is to avoid writing about computers, but rather the people behind them. Research for the book 'DarkMarket' involved many hours of interviews with hackers. They were all fascinating characters and this research led to some insights into what hackers can do, who they are and what their motivations are.

Sun Tsu, the 3rd century Chinese philosopher and military strategist, wrote "know your enemy". This simple message is very relevant to cyber security. Who is the enemy? What is really known about the hacker? Is there a working taxonomy of them? Who are the masterminds behind the attack? Is it suave social engineers, highly skilled hackers or psychopathic characters that combine both talents? Is there a highly abnormal instance of Asperger and other spectrum-related disorders among hackers? And if there is, what does it mean? Have traditional organized crime scenes moved onto the cyber world, and if so, why and how? If the ability to employ violence is essential to the success of the traditional organized criminal groups, is there an equivalent criminal enforcement strategy emerging in cyber

space?

There are plenty of anecdotal opinions about the nature of hackers. The security industry is obsessed with analytical tools in the digital sphere, but it is also important to know what goes on in the human sphere. The majority of ideas discussed in this conference primarily involve a practice of social engineering. Criminals or other types of people, persuading people to do things with their computers that are not in their interest - this is not a digital issue, but rather a human issue. Hackers are very clever people and they have learned very quickly that the quickest way to persuade somebody to do something that is not in their interest is the promise of sex. For instance, there was the 'I love you' virus, which was one of the first viruses that spread fast around the world.

Not enough research is being conducted into how these people think in terms of manipulating human psychology, but research is made very challenging by the lack of consensus when it comes to definitions. The term 'hacker', for example, has undergone a remarkable transformation over the past 20 years, from a largely positive to overwhelmingly negative. Yet, the essential activity of hackers - exploring computers and their network systems and establishing vulnerabilities - has not changed. Researchers tend to argue that it is chiefly law enforcement and the media that have repositioned hackers and hacking in this way. Mass media presents a big problem in this regard. The name "hacker" has come to be applied to anyone involved in crime that is cyber-related. For example, the Murdock scandals were habitually referred to in the British press as phone hacking. Certainly, the journalists involved exceeded their authorized access to a system. They did so by bribing police or providers to give them PIN numbers of the voicemail boxes of celebrities. You can see why it is referred to as hacking, but no computer skills were involved. There is therefore a problem with definition.

The people who would be understood to be hackers are people with very advanced computer skills. This is a very new type of person, with which the criminal justice system has not really come to terms. The following quotes all come from interviews conducted with former or currently active cyber criminals.

- "So basically, I can send a message from anybody's cell phone to anywhere in the world and I write what I want. I had a lot of fun with it."

- "The great majority of those cradlers who were arrested were

either young, naïve or careless; as far as I know, none of the powerful syndicates of the Russian groups have ever been detected or arrested. My sense is that the Feds don't even know who they are."

- "The most basic rule, as far as I am concerned, is never ever touch American cards. It is not because American cards are difficult; they are the easiest in the world. It is because if you do American cards, then you're under the jurisdiction of the FBI and the Secret Service. Canadian and European police I can handle, but I prefer to stay away from the Feds."

- "We were not born yesterday. We are serious operators. We have a digital and a human intelligence capacity. The FBI may be watching us, but we are watching them in return".

The counter-intelligence capacity of the hacking community is more advanced than people imagine it is. They have contacts inside many law enforcement agencies. They are able to exploit competitive divisions between agencies engaged in cyber investigations. The recent case of anonymously intercepting a recording of a conference call - consultation between FBI field officers and the Metropolitan Police cyber divisions - has demonstrated that carelessness is not restricted to young carders, but characterizes cops as well. In the past month, evidence has emerged from a confidential document of the UK Serious Organized Crime Agency (SOCA) that was leaked in Britain. The private investigators working for organized criminal syndicates employed hackers to breach the network systems of three of Britain's police forces. This is further evidence that traditional organized crime groups are beginning to appreciate the value of cyber capacity.

As always happens in a recession, established syndicates turn to fraud. On the occasion of the collapse of Lehman Brothers in 2008, when they turned to fraud, they discovered that the Internet was transforming the scale and nature of fraud. Elsewhere, the Mexican cartels now possess a sophisticated digital backbone that expedites their business - shipping cocaine into the United States from South America, and which is also used in order to monitor and assess the capacity of their domestic opponents. Bloggers that had sought to expose cartel activity were tracked down via their IP addresses and murdered last November. The use of violence in cybercrimes is still rare, but as they further develop their surveillance capacities as indicated above, the incidents of violence are likely to increase.

Assessing the actual cost of cybercrimes is quite simply

impossible. With no legal obligations to report breaches, the picture will always be horribly incomplete regarding the damage that cybercrime inflicts. This of course does not stop people from making dramatic claims all the time about how much is lost to cybercrime. The White House claims that it is one trillion dollars. However, this is just a guess. It might be more; it might be less. Looking at this problem from the opposite perspective is instructive. How much is spent on cyber security every year? And what is it spent on? The London-based business consultant Visiongain has estimated that Western governments spent 37.9 billion dollars on telecommunication cyber security in 2011. Then there is the private sector. Gartner calculates that for 2011, the total spent on both software and services was 51.4 billion dollars. The US, Western Europe and Japan make up 75% of that figure, so the current total cost to governments and industry is just shy of 90 billion dollars. This does not include China and Russia. It can be safely guessed that these two countries spend around 10 billion dollars. This is roughly how much the industry is worth every year: one hundred billion dollars.

Additionally, the estimated compound growth rate will fluctuate between seven and eight percent in the US, Western Europe and Japan. From this, it is clear that the cyber security field is not significantly negatively impacted by the economic crisis. In emerging markets, this compound annual growth rate is calculated as high as 15%. Most of this large amount of money being spent is going to high-end technical solutions for cyber security. The industry is interested in research and development projects that are channeled into product development. Given the logic of the business, the industry simply does not care and is not interested in devoting time or money into getting to know the enemy. Our government is not demonstrating any interest in the opponent, while some governments are, but not necessarily in the way that we would imagine. Here is an interesting point where cybercrime, cyber espionage and cyber warfare intersect. Research for the book 'DarkMarket' had led to investigating the website 'Carder Planet'. This website was founded just after the turn of the millennium, and was the website that changed the face of cybercrime. 'Carder Planet' had introduced an escrow system that enabled criminals to overcome the primary challenge facing them all, which was how to trust the person with whom they were doing business when that person was a criminal and untrustworthy. The escrow system was as joylessly successful as a venture, that 'Carder Planet' finally organized the first-ever

worldwide international "carders" conference, which first took place in May and June of 2001 in Odessa. Carders came from all over the world and held plenary discussions in the hotel Odessa and breakout sessions in various restaurants around town, discussing subjects like how to better exploit the smaller cards. In a press release from the worldwide international carders conference, the first item on it was particularly interesting:

"Once again, the critical issue of the inadmissibility of any action in relation to the billing systems, banks or other financial institutions in the Commonwealth of Independent States, especially Russia, Ukraine and Belarus, was raised. The family will deal ruthlessly with any carder found engaging in such activity."

One of the founding members of Card Planet has revealed that the deal with the SPU in Ukraine and with Russia was explicit: carders and other cyber criminals were free to attack anyone they liked in Western Europe and the United States, but woe betide anyone who launched an assault on an institution in Russia. The second part of the deal was that should Russia require hacking capacity for purposes of national security, then the criminal hacking community would be expected to make its contribution. This was precisely the case in the 2007 attacks on Estonia and 2008 attacks on Georgia.

The Chinese government also mobilizes the cyber attacking community for specific political aims. We have finally entered a world in which states are willing and able to deploy cyber-attacks on behalf of their national security interests, outside of any regulatory framework. This is only likely to proliferate, as the chances of Russia, China and the United States reaching an agreement on a global framework is very unlikely.

Large sums are being devoted to military and espionage. However, it could be argued that governments are struggling to meet the enormity of the challenge in cyber. They are hampered by bureaucratic procedure and lack funding. Research into the human aspect is not high on the priority list, if it exists at all. Apart from trying to introduce practice and basic cyber security techniques in state institutions, governments driven by policies of austerity are increasingly relying on evermore-draconian penalties to deter those involved in cybercrime, cyber industrial espionage and cyber warfare. This has nothing to do with knowing the opponent. It is instead focused on investigating, arresting and prosecuting those who are in the terminology of the US Cyber Fraud and Abuse Act exceeding their authorized

access.

If there is to be progress with the issue of cybercrime and cyber security, then these fields can no longer be left up solely to law enforcement officers and technical specialists. This is now something that requires criminologists, psychologists, anthropologists, lawyers, journalists and a large variety of people to understand. To this end, I will be working with the citizen lab of the University of Toronto to set up a project designed specifically to research the community of hackers around the world, but also to engage with them. Understanding hackers and working with them is the key to solving the human problem behind this extremely significant major technological issue of our age.

Managing Advanced Security Threats Using Big Data Analytics

Mr. Ed Schwartz | VP and CISO, RSA, Security Division of EMC

We will discuss here a concept called intelligence-driven security operations, because it really is about knowing your adversary. There are significant gaps in security today and the question is how attackers see the defenders; how networks look in the face of hackers, cyber criminals or state-sponsored organizations. Most notions of defense are based on some notion of foreign knowledge of attack. The 80% of known low-level attacks is a basic threat that must be addressed. Unfortunately, there are many adversaries focusing on the 20% that are unknown and very advanced. A more advanced capability must be developed to deal with these threats.

Last year, a study asked 12,000 security folks in the US and in Europe how long it took them to detect an attack. The average answer ranged from one week to 60 days. The advanced adversaries out there today have the potential to do a lot of damage within a time frame like that. As disturbing as these statistics are, the truth is likely a lot worse. Prevention is not an adequate strategy. There will likely always be a certain level of exploitation. How does one plan and create an environment in which damage is limited to a level that is reasonable and manageable?

A conventional threat considers two men with ski masks and flashlights as bad, and as a threat to be focused on. However, the cyber reality is more similar to a stadium full of people all dressed alike and looking normal. This presents the mathematical challenge of trying to figure out which is the person that has the explosives tucked in his clothes. This is a problem that requires

other skill sets. More data and analytics are needed. After the RSA's security breach last year, the company's defensive model was changed to really put the adversary first.

Intelligence must be gained as to who the hackers are, the likelihood of attack and what they are after. Organizations must understand that not everything can be protected equally and that resources should not be spent attempting to do so. Earlier in 2012, RSA and EMC were not considered a target for Anonymous; but a few months ago, RSA supported a certain piece of legislation, and all of a sudden became a target. The landscape is constantly evolving. In order to be ready to make the necessary changes, one must consider the capabilities of the adversaries, what means are available to prevent them and what means there are to detect. Operational intelligence is necessary as to how they view an attack surface, in order to understand delivery or weaponization. Most organizations do not understand an attack until it is deep inside their network or until they see catastrophic losses.

The interesting part of defensive solutions is that as the cost to remediate problems goes up for everybody, the attacker also has an increased cost because the exposure level goes up. As the cost of the attackers goes up, they move away from automated processes and change approaches. As they move to lateral movement and other types of directed attacks, they become much more visible - if defenders operate properly. This means building the right processes, gaining the right data, and all with the right people. There is a high detection potential with great opportunity that is under investment in the cyber security world. There is an opportunity for innovators to build startup technologies, to build service companies; an opportunity for a building process; an opportunity for success in terms of winning over the adversaries.

There are three characteristics to discuss in terms of how one views technology, security programs, and approaches to take in hiring companies like RSA, in terms of internal programs. Contextual, risk-based and agile are the three characteristics that are important for any program today. There is a popular equation from security studies: $\text{Risk} = \text{Threat} \times \text{Assets} \times \text{Vulnerabilities}$. This is an unsolvable equation for a number of reasons. First is the impossibility of quantifying 'threat'. As for vulnerabilities, a company could determine it has 23,000 vulnerabilities, but after scanning its network, realize that it has more. Those can

be patched and then Adobe can come out with a new version of 'Flash'. How does one determine if this is good or bad? It is more effective to look at mission-specific material assets that matter to the organization. Only in this way is there a real chance of protection. How containerization, virtualization, mobility and cloud-based assets relate to the attack surface is the key.

Social presence has been discussed. How the entire surface looks like and how it relates to those assets is connected to which adversaries want those assets and what capabilities they deploy. This creates a more realistic and workable equation. Contextually, most organizations today in the US are not focused on this. For example, the last network technology that most organizations bought is Intrusion Detection. They are analyzing logs and trying to figure out why the logs are not notifying that criminal groups are penetrating and stealing assets. This is because the logs are not attenuated. A lot more data is needed. A Chinese philosopher wrote "when the trees move, the enemy is advancing". This means that this is about knowing our networks and our adversaries better. Network logs tell only a portion of the information. In addition to logs, there are physical security data, HR data, full package data and asset management information. Networks would tell so much if organized properly and given a security context. The next step would be performing statistical analysis or analytics on this new data. There is also an entire universe of external information from the government, information from market sectors and open source information. If this is then distilled and fused with internal information, the results could be tremendous.

Kill chain methodology is a great methodology. Most efforts to detect adversarial changes in the kill chain look for people scanning for or making opportunistic attacks or network layer attacks, or for people looking to exploit vulnerable protocols. Today, though, something else is happening. Attacks are open-source-based, targeting 7 layers, and cyber security has attenuated neither technologies nor processes to look for this. This is much more difficult and requires a lot more data. It requires a different approach. Multi-source intelligence means knowing the adversary, understanding who out there has information that might be valuable to me. Cyber security professionals cannot sit and wait for the government and others to figure this out. Private companies cannot go and figure it out on their own; neither can a government agency. What RSA has done is to work with vendors, partners, and create data sharing relationships. There

are vendors that can provide answers. Sharing information is the start of an eco-system. It is a beginning, and nobody can know just how far it will take a company or the industry in general. This is an example of what Big Data can do for a company.

Insider threat management is not such a clear issue anymore. It could be a user, a spy or a compromised device or process. A risk scoring methodology must be applied to big data from internal and external sources and designed to intersect all these vectors. An action such as a contractor with 30 days left on his contract inserting a USB drive in a PC while connected to corporate VPN should be recognized within moments of occurring. This is very possible today. If all this data is combined and fused, it enables arriving at many conclusions relatively quickly.

Finally, it is important to discuss agility, which includes four basic ideas. Comprehensive visibility means know everything that is going on. Analytics must be open; standards must be supported openly - open support of any kind of data being brought in. Systems must be connected to do link analysis. Actionable intelligence is necessary immediately. Waiting 8 hours for a query to come back means deep trouble. Doing incident response the same way as 2 years ago will lead to failure. Architecture is important, including what the back end looks like, what the entirety of the storage situation is, and how to normalize hundreds of data elements so that a user ID is a user ID across hundreds of systems. This is a data scheme issue. One needs to think about combining analytics so that there are not 10 different analytics platforms, but one that works together with all the other components. How does this architecture enable preventive systems and how is information fused and enriched using all kinds of threat intelligence across a life cycle of information?

Better analytic skills are needed, as well as big-picture thinking. How do we get all of these characteristics? An incident response team should have many varied types of skills.

In closing, prevention is impossible and organizations should therefore think about reallocation of resources; move away from spending everything on prevention. There should be a balance between prevention, detection and preemption. It is important to focus on the adversaries and understand them better. That is the information that should be tied to material assets and the mission. Security is a Big Data problem and one that requires planning. Anyone scared by terabytes should get over that

immediately. Intelligence must be fused into the problem. There should always be at least 3 ideas behind everything done. Not thinking differently about this problem will lead to failure.

Hacktivism Comes of Age

Mr. Avi Chelsa | CTO Radware

Radware specializes in two categories of products: Load Balancing and Network Security. The company focuses on behavioral analysis of networks and applications to find anomalies and attacks.

Long term tendencies need to be considered. In the last decade it's evident that - there is a change in the motivation of attacks. It began with acts of vandalism, hackers tried to make a point- that they were good and knew how to evade detection and how to crash applications and steal info. 2003 marks the change in attacks' motivation and since then they became real cyber crimes. Cyber crime organizations have grown and become capable of crashing almost every network. Motivation wise, Radware has an ERT team whose task is to research and question customers about trends. From a motivation aspect- hacktivism is an important issue.

To summarize these trends, the field began with known worms. Later, cyber crime started using DDoS to attack service providers in order to crash their service. Recently a new challenge is occurring: the attacks become a blend of different attacks, hence it's a greater challenge protection- wise.

Its beginning was in 2009 with attacks on eBay and Visa/ MasterCard; and in 2011 it changed direction and became known as "Advanced Persistent Threats". It's so challenging because those attackers, these multi-vulnerability attack campaigns, create a long -term simultaneous attack operation directed at several systems or layers on the networks and servers alike, hence the name "multi-vector attack". Not only do they cover a

small number of protocols on the net or application, but also they cover all possible protocols. Meaning, all possible applications are being attacked. It creates a new challenge to the defenders, since they specialized on a specific application or protocol and know how to protect it, and now it has changed. A good defense needs to collect all these capabilities.

A little background on the advancements of the realm of hacktivism. If I'm referring to 2009, then it kept on moving forward. It started from something very basic, volunteers were recruited and told to come and construct whatever attack weapon and use it to attack certain organizations. For political reasons it became more and more advanced. Today we see a complete operation. As I've mentioned all sorts of attacks are used, simultaneously. Usually the organization decides on a specific target; studies it for a long period of time, and performs so called proof firing to avoid detection in order to learn what tool is best suited for their task. Then time is decided upon, and at the best time when the organization is most vulnerable they attack. This is the way an attack is carried out. Most of the people the organization uses are not experts. But there is always that hardcore, a very professional and strong group that knows how to conduct it. Another interesting thing that indicates development, and here I'm talking in quantities, is the overlook at various parameters that provide measuring of how advanced is the attack. As you can see, some two, three years ago the attacks on Visa and MasterCard lasted about three days and included a total of four vectors, different categories of threats were launched at these websites; those attacks became more and more advanced, not only at the level of the attacks but also at the level of the length of the attack. When the Vatican was attacked the significant attacks lasted twenty days. This demonstrates the challenge of these organizations; the organization can't just rely on technology. Twenty days implies that it has to have a resistible reaction power; long term resistibility. The attacks combine also intelligence gathering attacks and it lasted several days. The websites face today diverse large scale attacks that often fly below the radar of the monitoring systems. We ought to be prepared for that.

Israel sustained at the beginning of 2011 attacks from hacktivists on government, banks and stock exchange websites. You are going to see what I've already said before; every time they said "what's the problem? It arrives from a specific country, let's do the Geo IP blocking and be done with it". This privilege doesn't

exist anymore. Now it comes from everywhere. The threat is not only an external one but also comes from within. I believe it was mentioned before several times and that's why the concept has to be changed.

What does changing the concept mean? We cannot, as already said but I'm going to stress it, we cannot rely on knowing somebody. That fact that it comes from within Israel implies that there are many machines, computers, cellphones that are already infected. They are infected and it's about such users that might be part of the organization's customers, users or employees; and we ought to conduct a behavioral analysis, not in order to identify them according to those characteristics but to understand if they behave any differently than how they used to, and by so doing to understand if they are infected. These are the kind of things we do at Radware. A little about trend from the industry point of view: as you see, the main trend as hacktivism goes, as targets go are governments. There were others as well, but I believe that governments or government organizations are the main target of massive attacks. To sum up what we think: we ought to advance in the cyber field. There are three criteria we work by: the first one is sharing info. A lot was said about it in the past. Radware takes our equipment that knows how to analyze and also do a deterministic and behavioral analysis, distribute them to the clients and the service providers. That way, as experience taught us, we can really protect our clients better. There are certain defenses that cannot be implied if the client is too far. You don't have the intimacy of his applications, the users', every user's behavior; you can't be attentive enough. Therefore, the systems have to be much more in proximity to the customer's services and implications. And in order to defend from larger scale attacks and do it properly, equipment has to be installed at the service providers- not only in Israel but abroad as well. Automatic channels and teams be synchronized and work together.

Another very important criterion on which, I believe, nothing was said: counter intelligence was discussed, but counter attack was not. At present we are very much in focus, we want to focus on analyzing our hits, the applications, the nets and try and cover them, close it with all sorts of defenses. In a more advanced way, more pro-active or less pro-active way, we are looking less at the attackers' vulnerabilities or limitations. Attackers use all weapons. For the attack to yield fruits they need to attack using their attack strategy. The limitations can be analyzed and while

attacking all sorts of signals that can slow them down and make them disappear, can be launched. It's very important in attacks' campaigns. How will you do that? By using technologies that covertly begin to block their attack tools. Then they might decide to move to another place. It's a war of attrition.

The last thing I want to say is that part of counter attack or of any defense layout is, in my view, the fact that a lot of research in the field of preparation, policies and such is done here- all those things that a lot was said about here, forensics; as of capabilities- there is a big potential here. Of course we ought to improve, but there are good capabilities there. The need to include all experts of all fields- applications and networks- experts that know how to fight a counter attack while an attack is ongoing, is something less focused on; this is something we are trying to advance: the skills the team needs- the response team while an attack is ongoing. We need to know that as is in the military field, the front line of defense will always be breached. And at this time the fate of the attack is in its hands, and it's the team who ought to respond, a swift and powerful response.

In conclusion: from our perspective, we believe it's the cooperation that ought to be pushed forward; an overall view above content, policies and behaviors is needed. Also the issue of abandoning the focus on solely protecting and moving into counter-attacking is also very important; as is of great importance that those response teams will have sufficient training.

The Dark Alleys of the Virtual World

Mr. Menny Barzilay | Head of IT Audit, Bank Hapoalim

The virtual world is a different dimension. When we are in that world, laws of physics work differently as does our psychology, and there are other social aspects in that world. In order to know how to get along in that world it has to be understood. Even though in certain places we are trying to blur the differences between the worlds and use the physical world terminology in the virtual one. We are told that if we behave in logical reasonable manner, everything will be alright.

The question is according to what logic we are expected to behave? Can the logic we use here in the physical world serve us there in the virtual one? Is a dangerous thing here is equally dangerous there? The more we understand the difference between what is real and what is virtual, we'll be able to understand better the dangers lurking in that world, we'll succeed in better developing the correct strategy for coping and better grasp the opportunities given to us.

The brain's right side is the creative part whereas the left side is the analytical part; and I always keep on asking the human resource people and others on which side of the brain security info is. We ought to develop a virtual awareness in order to understand who to deal with in that world.

At first I wanted to say that not knowing to think virtually was like living in a world in which you couldn't fly, without knowing how to fly. Then as I thought about it I developed the another metaphor: living with virtual consciousness was like living in a flyable world without knowing that there were actually people who could fly. However what I want to say is that living in the

virtual world without virtual thinking is like living in a flyable world with the word "fly" excluded from the vocabulary, without actually grasping the meaning of flying. And when you don't understand you are actually living inside the box.

In order to think virtually, we ought to courageously develop awareness. One needs courage to re-ask basic questions. How do we measure power? Supposedly, in the physical world the answer is quite simple and in the virtual world it's intricate. The virtual criminals are not the ones we're used to seeing in the physical world. Crime was not their last resort, they are not people who could not integrate within formal frameworks; they are completely normative people. The most brilliant brains of our era turn to cyber crime since crime psychology in the virtual world is different from the crime psychology of the real world.

You don't get out of bed to commit crime; no blood to be seen; no-one points a gun at you; no one is chasing you; no cars pursuits. As a matter of fact the most amazing crimes can be committed from the same place one prepares one's homework. And if something happens, the computer can always be turned off, lights switched off and sleep at home. No need to run.

There is another dimension that creates different kind of criminals in the virtual world and it is the way those criminals are perceived. Whereas the real world criminals we want to denounce, the virtual world criminal are heroes. For instance, someone breaks into a bank at night and robs some 60,000 Shekels – he is a thief. We'll demand to incarcerate him and try to protect our family from him. But at the same night a hacker breaks into the bank's servers and steals some 60,000,000 Shekel; we'll regard him as a hero and put the blame on the bank's info security. It's great fun and more gratifying to be that kind of criminal.

An amusing difference between the criminals in this context: if someone goes to jail from crimes committed in the physical world like robbing a bank- when he gets out his options in life are quite limited; however, if someone goes inside for committing computer related crimes- he gets out and gets a consultant job. Is "boundaries" a real world word? Is the virtual world a place or a country? If we ask fourteen years old kids whether PayPal is in the USA or Europe, the answer is will be "in the Internet". And if tomorrow PayPal decides to move from the USA to the Far East, will it matter to anybody, should they know about it?

There are interesting questions to be asked when the discussion evolves around the notion of a country. What in effect is a country? A country is a group of people with some physical

territory that have decided to behave according to a certain set of rules and defend themselves. Is the physical territory important within this definition? In other words- is there a possibility of a state over virtual territory? The virtual world provides people the opportunity to group not according to their place of origin but according to another set of beliefs. For instance, a "The Simpsons'" lovers country can be founded, or a country of animals' rights' activists who will attack anyone who doesn't have the same views.

The question of how we measure power has become more important. We are accustomed that power can be quantified, like whose army is bigger, hence to know who is standing in front of us and how to deal with them. The greater the dependence on technology is so the power of the state over people diminishes. People obtain more power and groups of such people fight states.

The states face the question of how to counterattack these groups: Wikileaks versus the US battle, or Israel versus the Saudi Arabian hacker. The more our dependency on technology grows, so will the country's power diminish.

There are also hackers capable of killing people with a push of a button and turn off entire electricity infrastructures and cause enormous damage.

The virtual warfare between countries derives great power from cyber crime, cyber infrastructure and has the financial resource. A place where money is found- is a place where crime is found. Crime creates additional tools in the front of warfare amongst countries or organizations. The important question is how to measure power. We can say that in the virtual world we all have equal power since we can rent the necessary services. We are living in a changing world. The differences between this crime infrastructure and the citizens and state are blurring. We are living in a world in which Iran has a big interest on spying within Google or Facebook.

The better we distinguish between what is real and what is virtual, the better we'll be able to think virtually and better capable of developing the strategy of coping with this world. If in the physical world there is one truth and that is that Man is mortal; so in the virtual world there is one truth and that is that if it is connected to the internet- it can be hacked.

Catching the Bed Guys - Lurking in the Hidden Cyberspace

Mr. Guy Mizrahi | CEO, Cyberia

We have a three dimensional perception of the cybernetic space: the physical, the logical and the human dimensions. Cyber is a huge intimidating thing; we all regard the internet as something nice, a place where even our children play in. Actually, there are many nasty things going on there, like groups who seek to harm countries, organizations and people. Why then use cyber attack and not other means? Cyber is a strategic, cheap and available weapon, easy to buy and obtain and with a great damage potential.

An effect of ambiguousness envelops the cybernetic world. Trojan Horses cannot be counted like tanks and planes. Attack's origins cannot always be identified and deniability always exists. Assuming origins of attack can be located, is it really possible to identify who is responsible? Are cyber weapon anonymous? In the cyber crime world, things can be checked in a somewhat more interesting way and I'd like to test two theories: the first one is the Koobface worm that stole among other things FTP accounts, Facebook accounts and more. When the worm was activated - the people responsible for creating and operating the worm were caught. How this operation was carried out and how were the responsible found? A thorough examination reveals that attackers made mistakes along the way. For instance, they activated various services that shouldn't have been activated there. They let the public have accessible backups, but the most significant thing was that they operated using the usual codenames and did not disguise their identities, they used their personal cellphones for reports and accidentally left their own

personal photos in the servers after the worm had become operative. Through one of the pictures one member Facebook account was discovered and they used the same cellphones for both personal and "business" purposes. The usage of the same nicknames for personal and business and crime matters and the mixing of the real world with the virtual one was their downfall. For example, one of them directs to a website and an unexplained number appears. When analyzing the number we can see that it's K0600 and the 078 and RUSS. Primary analysis says Russ is probably Russia. 078 may be area code. Solving the meaning of K0600 remains. After checking and searching, the responsible man's blog was identified and the person assumed responsibility for acting against Georgia. There are strong suspicions that the government that wanted to harm Georgia perpetrated the attack and the hacker was operating under direct orders from the government.

Conclusions: a cyber attacker can remain anonymous and methodology is very important. Modus operandi has to be such that won't enable detection and leaving no room for errors. Therefore, a hacker ought to be organized - and I don't know any such hackers. A different sort of management is required, therefore the one to be in charge in most likelihood won't be a hacker.

Cyber warfare requires different capabilities, multidisciplinary, IT security, and hacking. These are work tools needed to execute cyber warfare in the best possible way. If we comply by the regulations and accepted norms of operation we might remain anonymous. An investigation of the cyber events and research methodology for cyber events is needed, since even in the cyber world - the perpetrator can be discovered.

03

Third session: technological Aspects of Cyber Security.

Cyber Security Lessons from Fighting Piracy in Pay-TV

Dr. Abe Peled | Executive Chairman and Chief Executive Officer, NDS Group Ltd.

NDS was established in 1988 to look at applications of encryption. When pay-TV became a target for piracy and hackers, the company converted to handle that threat. Today, NDS provides security systems for pay-TV operators worldwide, protecting over 50 billion dollars of revenues as well as a host of enabling technologies. The critical security technology comes from Israel and the company employs approximately 1,400 people in Israel, mostly in Jerusalem. NDS works with pay-TV operators worldwide and it is relevant to this conference that pay-TV was one of the early intellectual challenges for hackers. The first hacker that broke the sky signals was a graduate student that wanted to see the film Star Wars but could not, and therefore broke the system. It was quickly realized that money could be made out of this, and thus more people embraced these techniques. In the early 90's, this was the scourge of the industry. It threatened the whole existence of what was a very young industry.

Most hackers lack any formal education and they had perhaps started doing it for fun and then realized it can be capitalized. The arrival of the internet and the ability of hackers to communicate

and share techniques internationalized the hacker business and attracted the best and the brightest of that time into this industry. In 1995, it was clear that cyber security technology could be improved, but that that would not be enough because the issue was more complex. In the early days of NDS, Reuven Hazak was recruited as Head of Operational Security. He came with expertise in intelligence and helped to develop a three-step approach that helped to eradicate piracy in the pay-TV industry. The first step requires acquiring the best possible technology that is affordable. Cyber security can be built like Fort Knox, but not many people can afford it. The technology must be affordable, but it must also be constantly updated, because the threat is constantly changing. Part of this process involves getting to know hackers and how they think and co-opting some of them to teach engineers how to design systems that could not be hacked. The average PhD does not think the way hackers do. Hackers are basically self-taught, autodidacts, and they think completely non-linearly, in ways that an engineer would not think. For example, an engineer would not apply a 50-volt pulse to a chip that should only receive 3 volts to see what happens. An engineer does not do this because he knows it is a 3-volt chip. Hackers challenge traditional methods. NDS had to learn from them and had them train designers to use these methods. Additionally, the company established a team called the “Black Hat” Team in a separate location. This team tested the company’s systems using hacker methods. It was deliberately located in a different place so as not to taint the concept development with the same ideas. A company should constantly evaluate itself as an opponent would.

Intelligence gathering and constant monitoring: There are not many people that have the intellectual capacity, the interest and the capability to penetrate these systems. Finding them is key, rather than building an ever-higher wall that is used by the millions of people. Finding the architects, the generals, is necessary and ultimately possible because their numbers are small. Hackers usually have big egos and therefore have networks in order to achieve the recognition of their peers. Following the money trail is important, but one should remember that for hackers, it is not just about the money. These networks need to be infiltrated. NDS has established a unit that can communicate on a native level in 14 languages, because hackers are international and can immediately detect an imposter. This unit functions to understand what hackers are up to, what the next threat is and

where it is coming from. The unit also discovers the techniques being used in real time in order to combat that threat.

Cooperation with law enforcement agencies is essential. Prosecuting pay-TV piracy is not glorified and does not get prosecutors appointed as Attorneys-General in the way that catching a serial murderer does. It is not a high-priority crime and people are not sufficiently educated on it, so NDS spends a lot of effort on education and training. This preparation aims to help create a 'silver platter' on which to present cases so that they can be prosecuted.

No particular product is a silver bullet in cyber security. NDS monitors attacks and the attackers and conducts counter-attacks. I think one of the speakers talked about the importance of counter-attacks. The best defense is offense. The offense can be technical in nature; but offense can also include spreading information on hacker forums, penetrating hacker networks and making them suspicious of each other. Understanding who hackers are is critical. A defender must appreciate how hackers operate, how they might attempt to penetrate organizations and how people from inside an organization may become seduced by being part of it.

In the case of NDS, the result was positive. Traditional piracy in NDS systems was eradicated completely. However, technology does not stand still; there are constantly new threats. Hackers never try to penetrate the most difficult target, but rather look for the weakest link to attack. In this light, NDS has shifted focus more to internet intelligence, identifying those obtaining illegal programming in the first place and shutting them down. Identifying hackers is necessary, as is co-opting them. Dealing with criminals inevitably creates some unpleasant issues; and it is worth keeping in mind the adage that sleeping with dogs, one may catch fleas. However, the industry does not have the luxury of not understanding the hacker community, as it is a potential source of effective intelligence.

The legal framework is always lacking in terms of supporting proactive activity. This is not only an issue of priority, but rather the actual legal framework. Rapidly evolving technology and the popular view that 'content should be free' impacts these frameworks. Further, one man's hacker is another man's hero, depending on what the hacker does. Some would say that if a hacker broke into a Chinese government network to find information about Tibet activists, that person would be hailed as a hero. The same technique can be used to steal money from a

bank, and then that hacker would be a villain.

A lot of the discussions focus on technology, monitoring, and erecting ever-higher barriers. Organizations want to be able to look at logs and extract intelligence. Such technology and applications are necessary conditions for cyber security. However, progress in the technological arena must be complemented by proactive intelligence gathering, by understanding who hackers are and tracking them down. Understanding hacker techniques and in some cases co-opting them must be an integral part of the technological development of solutions and of the service being protected.

In cyber security, the commodity in shortest supply is expertise. Expertise is not simply a tool. There are 300 different products, software systems and technologies that one can buy today. In every penetration test that NDS has conducted, the issue was not the lack of appropriate tools; the issue was that the customer did not implement them correctly or monitor them correctly. The ability to centralize this expertise and deploy it on a worldwide scale is a big opportunity for Israel. Israel has the expertise, cleverness and deep insight necessary. It now has to translate these abilities into a business model that will create a service combining the three main elements of cyber security as described above.

X-Force Trend Report 2011

Mr. Martin Borrett | Director of the IBM Institute for Advanced Security Europe

The Scaliger castle in Northern Italy was built in 1151. At the time, it was absolutely state of the art, the very latest in castle technology. It had very thick stone walls, over a meter thick in places, with square turrets. It stood undefeated for 100 years until 1251, when something disruptive happened. Gunpowder was introduced to Europe, and with it came the cannon; and this particular castle was overrun. At the time, robust square turrets were considered a good idea, though it ultimately led to the defeat of the castle, as they were the perfect target for cannon balls. After this time, castle design evolved. People built castles with round turrets and other ramparts and defenses to protect against cannon balls. This serves as a reminder that security is an ongoing process. There are always new threats and more challenges around the corner that demand rethinking approaches. Coping with new demands requires flexibility and agility. Architectures need to be modular and adaptable in order to adjust to the challenges of tomorrow.

There is no silver bullet in cyber security, as has already been pointed out. It is important to look at a combination of people, process and technology when addressing cyber security. A good thing to open with is a definition. For IBM, cyber security is about protecting organizations and their assets from attack in order to minimize the risk of business disruption. This may seem like classic information security, and a cyber security professional will seek the 'cyber' in this definition. IBM has been spending a lot of time talking to clients about a concept called 'smarter planet', which will help put this definition into context.

Smarter Planet is about the way the world is changing, as is the fabric of the infrastructure that is relied on every day. Technology has crept into the fabric of everyone's lives. By this, we refer to the way in which devices are increasingly instrumented. Computers, laptops and smart phones are only a part of 'smarter planet', which extends to all sorts of devices, some of which are not even recognized as computers. For example, the latest generation of heart pacemakers is fully instrumented. The new pacemakers monitor the performance of the heart, how it beats. They also monitor the performance of the pacemaker itself; and this information can be downloaded, logged and emailed to a doctor. The doctor can review that information, check how the heart is performing and how the pacemaker is performing as an electronic device and even reconfigure the pacemaker wirelessly as needed. This represents fantastic progress, but from a security perspective raises key concerns about the security of that protocol, such as how is it being authenticated. Pacemakers are only one small example of a larger trend that includes insulin pumps, cars and refrigerators. The trend of online interconnectivity extends to parts of critical national infrastructure that are relied on daily to distribute power or water and many other essential public services. This interconnectivity is the context of cyber security.

Threats are increasingly sophisticated. Cyber security now exists in a reality that is much more sophisticated and premeditated. Individuals and groups of individuals carefully research their targets using information often gathered from the public domain. The public domain includes social media sources, but information is also gathered by phishing and other intelligence gathering methods. Hackers carefully conduct reconnaissance, plan and do their homework. They find weak points in organizations and make an initial infection from which they expand out and ultimately go after their targets. This style of attack is typically long-running and requires patience on the part of the attacker.

Although much is known about attacks and technological solutions, there is no single IPS, firewall or technical control that can resolve this. The new threats require a holistic approach and looking at people, process and technology. Expertise is very important. IBM excels as a global organization with the necessary expertise and insight to handle cyber security, not just mainframes and software as is often associated with the company. IBM manages security in 133 countries around the world for some 4,000 clients generating 13 billion events

every day, which comes to 150,000 events every second. This is managed by 9 security operation centers around the world working together. IBM also invests a great deal of resources and millions of dollars in security research. In Haifa, Israel, the company does a huge amount of cutting-edge security research work. IBM works directly with clients, but also at international conferences, NATO, the European Commission, European Organization for Security and others. Only through international cooperation will some of these issues be solved.

One of IBM's leading security teams is 'X-force', which is made up of several hundred people largely based in Atlanta. This team was acquired when internet security systems were brought into IBM in 2007. They look at the overall threat and vulnerability landscape and publish a report every 6 months. After over ten years of doing this, 'X-force' has one of the largest vulnerability databases in the world. This enables IBM to compare and contrast what has been happening year after year. Some progress was seen in 2011. There was a decline in web application vulnerabilities and an increase in the number of patched systems. However, as security increased in one area, hackers found new and more sophisticated vulnerabilities to go after. Parallel to this development, the technology landscape also evolved. New technology platforms emerged, such as the cloud, people bringing their own devices to work, the increasing use of mobile in that context and social networks.

In the last year, IBM has worked to operationalize the approach to cyber security. Good and affordable technology is needed, but one must also look at the people and process aspect and consider how to operationalize it. Five key phases have been highly effective with a number of clients around Europe. This involves learning, situational awareness, preparedness, educating staff, security culture within an organization, security architecture, assets – everything to do with understanding and learning where an organization stands today. Then it is about monitoring, understanding what goes on in an organization on a number of different levels and then analyzing this information. Advanced security analytics is an important area to focus on, especially as gaining insight into the real-time context of a business or organization is increasingly becoming an issue of big data. Better analytics enable better decision-making. The ability to navigate around this life cycle rapidly involves having good processes, good communication and of course good technology. IBM has had some significant successes with

NATO, the US Air Force and the Federal Aviation Administration resulting from advanced analytics.

IBM is trying to take a holistic approach to security, and not to look only at any one dimension. We are looking across people, process and technology. The company has developed a security framework that has solutions focused on people, data, applications and infrastructure. Government risks and compliance are considered. These solutions are fueled by the research conducted. Security analytics and intelligence is going to become increasingly important for gluing this all together and gaining deeper insights into what goes on in real time. IBM is fortunate as an organization in that it can offer solutions to clients in several different forms: software, technologies and appliances that can be bought and deployed by the customer. There are services aiming to help with designing systems, architecture, self-assessment and viewing government risk policy. IBM has a critical mass of deep expertise that is nurtured in order to develop and retain that critical skill.

Trust No One- Information Security in a Hostile Environment

Dr. Eran Tromer | Blavantik School of Computer
Science, Tel-Aviv University.

I research beautiful software and algorithms that find their way to the real world where they start relying on all sorts of suppositions and believing all sorts of things that are not necessarily trustworthy.

We know this battle is in its infancy stage. The challenges are becoming bigger and more complex and we lack the tools of coping with them. Therefore, today I'll show some developments in basic research of information security and cryptography whose function is to cope with elements from the threats facing us.

We assumed at the beginning that internet cannot be malicious. As a community, we learned the hard way that we shouldn't believe anyone who linked in from TCP Port and from 1024 and by so doing, was trying to convince us he was legit. Traumas like Morris worm taught us that there were actually really bad people on the internet; hence we began to think how to defend against bad things.

So we constructed a firewall around the organizations' computers in order to block whoever was outside. It was very helpful - until we started puncturing the firewall over and over again with interfaces that were needed to link the organization to the external world. Consequently we had to add much more protection to the endpoint.

Maybe we trust the internet less than we trust other things yet we trust the software we are running, its credibility, whoever provides us with storage and information services, whoever provides us with external computing services, whoever provides us with

outside information, whoever is in the physical environment. We bestow a lot of unjustified trust.

Because the operating system is so complicated it's hard to trust it. Hence, separate virtual operating machines were implemented. Even NSA wrote a patent on the notion of creating two virtual machines, one with the secret key and another that runs a malicious code. It was great till we noticed that possibly the Hypervisor was not the right one. Somebody took control of the computer right at the initialization stage.

Software contains many risks, so are we to trust only hardware? Technologies that enable trust of the processor only and from there start building the required trust? This too is not true. I'll give two examples to show where the trust was broken. Where do software and hardware come from? Few headlines will sum up the argument of the chain of supply. For instance: turns out someone in China falsified chips of electronic components and sold them, with fat profit, to the American Army. While at it some transistors were changed too in order to change the component version number for purposes of selling it even more expensively. Such alterations in hardware can be destructive, can cause a complete failure of all security mechanisms actualized in the software that runs on the hardware. The military platforms depend on such hardware. The F-35, the masterpiece of the American Air Force, has 37 chips - not even a single one of them is made in the USA. What they are supposed to contain is known. But it is really all that is installed in them? Well, there are those who use Particle accelerators in order to peep into the chips to check the architecture. This is not an applicable solution that will allow us all construct our business and personal systems on the verified hardware.

Apart from the threats on the computing integrity, there are other threats. Let's assume we have great software that runs on some equipment. It has a secret key and it takes care not to take it out. But when this equipment tours the world, it falls into the hands of someone who measures the electromagnetic radiation emitted by that machine. That person plugs into the machine some measuring instruments of checking the computing intermediate value, checking the voltage consumption and looking at the light flickering in some LED bulbs. Attacks of that sort are known in the industry and literature as enabling the stealing of secrets from machines. In my research, we installed a microphone near some machines and recorded voices that were converted to spectrogram showing RSA signature keys. Additional software

for measuring contest on shared resources can be run on the same machine. Two processes run on the same computer. One is a malicious process measuring things like CPU and internal memory usage level; and the second process is trying to execute some sensitive operation. And then information leaks, because the sensitive operation causes a selective slowdown of the measuring process.

The malicious code can easily enter your computer. For instance, if the browser runs Javascript code - nothing more is needed. We can't trust the computer, not even in our own home; and we have no clue whether it's somewhere in the cloud. My colleagues at UCLA and I conducted an experiment: we paid some money to get virtual machines on Amazon Elastic Compute Cloud (Amazon EC2). We realized that it's possible to deduct where these virtual machines are placed within EC2 network. We showed that it's possible to identify where other machines are placed in the same network, and make our machines chase and catch until they all sit on the same physical computer. When two supposedly virtual machines hover in the cloud, they sit in the same physical processing core- we proved that a leakage of information from the victim's machine into ours can be caused, and then we collect and analyze that information. How did it happen? After all we teach students about abstraction and that each program runs in a virtual machine, that there is a complete separation. Well - these are fairy-tales. The resources are shared and unintentional leakage of information because of the competition on the same resources does exist. We are talking about actions on the level of few transistors inside a chip. Turns out some can exploit it. Then what do we do? The traditional way is to work very hard, to verify carefully each individual component in the system. It's possible; there are governments that have factories for manufacturing chips in order to be sure that what they are manufacturing is exactly what they have planned. But this is not a feasible solution because of its cost of billions of dollars.

I'd like to tell you about an alternative, coming from the realm of cryptography. Let's take for granted: we cannot trust anyone. Calculation will be disrupted, trust will be broken and each and every component needs to protect itself. How to survive in a friendless world? Cryptography enables the construction of big decentralized computer systems that allow integrity and confidentiality - a cryptography beyond the conventional cryptography of coding and decoding. Recent techniques allow complete computing through checking its accuracy and

secrecy. I'll present one technique from the confidentiality realm and another from the integrity.

Let's start with integrity. Assume an interrelated computer or component network. It's hard to verify that each individual component and computer does what it is required to do, hence we let pass that check.

But let's check what's going on amongst them. We'll demand a proof that the result of the computing that was done in that junction and the previous ones is accurate, and we'll do the same with every data pipeline. For example, an organizational system has two networks: classified and unclassified and we want them to be separate. To enforce the separation a "proof carrying data" can be added to all traffic flows. The final result of a computing that doesn't respect the separation will inevitably be with untrue and easily detected. We call it Proof Carrying Data, and at present it's being developed as a joint venture with the Technion- the Israeli Institute of Technology, MIT and Harvard University.

In the realm of integrity the example is an expansion of the notion of encryption. Fully Anamorphic Encryption is a recent breakthrough and enables working on encrypted messages. The idea is that the encrypted message will be sent in the same way a biology glove dispenser behaves: you can insert the gloves inside, play around but nothing comes out. Mathematically, that's how this encryption works: the secret information is inserted into such a dispenser with instructions, it's sent to the server and of course key is not included. The server can perform the activity inside the dispenser with suitable mathematical actions; compute according to the instructions and return the computing results - still encrypted. And from there, it can be decrypted. As I have said it's a breakthrough of recent years and we with colleagues from New York University and University of Toronto are searching for ways to improve and adapt it for cloud computing. Particularly it will be implemented in case a large number of clients are sending information, each one encrypted under a different key. We have demonstrated a simultaneous computing on two pieces of information providing encrypted results, while maintaining the secrecy of the keys' confidentiality. These are two proofs out of many for fascinating scenarios in which "trust no-one computing" can be performed. The techniques make trust redundant. They can make all computing safe. And when I say safe I am privileged to be formal: I can provide a mathematical definition of safety, an accurate model,

implying that these methods can be implemented in bigger systems. They are very strong candidates for changing the rules of the game in confronting cyber challenges, because they allow creating trust by computing encrypted data. I've mentioned at least one direction for using these algorithms but there are also challenges. First, there is the issue of the system's efficiency. Encryption can be done, but it takes too much time and more complex things become too expensive. We look for ways for improving performance and functionality. And most important, we are searching for the right applications that will let us see those things in action, contributing to real systems in spite of the efficiency problems. That way, we'll be able to focus our efforts where the immature technology already existing at present can make a real difference.

Qassams and Cyber

Mr. Michael Arov | Head of information security, R&D
Section, Rafael, Advanced Defense Systems.

Rafael, jointly with The Administration for the Development of Weapons and Technological Infrastructure (MAFAT) and the IDF, has been developing missile defense systems for years. Our cyber business inter connects with the physical world, especially in the realm of defense system. Iron Dome is the best example. Iron Dome was designed to provide a response to the Qassam's threat. The Qassam is a very primitive rocket: home-made metal pipe with explosives. Welding is not sophisticated either. If there is something to be said about Qassam - is that it's definitely not high-tech. Still, in order to intercept and destroy, Iron Dome has to be fast. The system is designed to intercept and destroy short-range rockets and artillery shells fired from a range of few kilometers and whose trajectory would take them to a populated area. The system is also required to respond to multiple threats simultaneously. It's a very fast, high-tech and computerized system.

Is there a real cyber threat on Iron Dome in view of the dissonance between the Iron Dome and Qassam? Of course there is. The operational scenario of Iron Dome is defending an area from short range surface-to-surface missile. The Iron Dome battery contains: Detection and Tracking Radar control center, Battle Management & Weapon Control (BMC) (missile control unit), communication unit and Firing Unit including several launchers. There is constant intra-broadband communication, since a lot of data has to pass very fast. The radar is scanning in search for launches. When a launch is detected, the system calculates the expected hit point according to the reported data,

and independently deployed while being operated remotely via secured wireless connection launcher containing 20 interceptors is chosen. This process is done in record times, negligible response time is obligatory.

Additional electro optic sensors are needed for this operational process. In addition all has to be multiplied for all interconnected Iron Dome launchers in order to get a full defense picture. In IT people language it means multiple complicated real-time processes, very hard to secure. Military equipment is as cyber sensitive as IT systems. The attacker wants to change the military equipment's function and destroy the system. Let's imagine a "Stuxnet" scenario directed towards Iron Dome – some malicious component causing uncontrolled physical explosion or preventing a launch. Hence, right from the beginning unique security solutions were integrated within the project. The cost was not negligible, but in spite of everybody, Iron Dome was delivered on time and successfully intercepts and destroys Qassams.

These are Rafael's conclusions from developing Iron Dome. Firstly, security solutions have to be implemented right in the very early stages of planning. Some of the solutions are possible thanks to prior planning and integration. Development time decreases as well, it cuts costs and most important improves operational performances. With all due respect to information security, the system's primary task is to perform the operational process. Secondly, a general overview on the complete process of information security is needed; the system's engineering integrates between the sometimes contradictory demands (mobility, resistibility, speed, range, timetable, and budget) in order to create a working system. Various solutions far beyond those of conventional engineering are able to provide cyber immunity. Standard immunity seeks to maintain the level of service in front of malfunctions and unexpected disturbances. In cyber immunity we ought to consider, on top of everything else, the enemy who thinks in a malicious way. Solutions like duplicating, standards compliance common in the standard world, are far from being sufficient in the cyber world. If a certain system is duplicated several times, redundancy is not created – it's still the same system. If a cyber-weapon is capable of hitting copy A, it can hit all other copies as well.

In order to comply with the project's costs and demands we have used commercial solutions. Some matched, some needed adjustments. Some of the solutions are uniquely ours. For

instance, in military equipment one cannot log out for switching a user. If there is ongoing activity, disconnecting for a moment to log-in and authenticate a user is impossible.

Systems are required to be cyber proof and we ought to give it our full attention. Such systems are possible to create, and we at Rafael are doing it on daily basis. We are trying to integrate as many commercial solutions as possible. It doesn't always work, but it's very important to utilize existing knowledge because there are plenty of good systems in the market. That being said, a full security solution by no means can be based on of-the-shelf products. Take a network, throw in some security solutions and hope for the best- it won't work. The whole picture has to be looked at, the solution has to be integral for the entire system. Thinking about ways to surprise the potential attacker must be guide lines, not only getting an answer via means of exiting solutions; security solutions need to be thought of.

The Need for Multi-Layer Cyber Intelligence

Mr. Mark Gazit | General Manager, NICE Intelligence Solutions, NICE Systems.

I'll talk about intelligence. Misha Glenny said here that whoever is involved in the cyber domain ought to be talking about Sun Tzu. It's rather interesting that someone who lived two thousand years ago sounds very innovative nowadays. Ehud Barak and Isaac Ben Israel's lectures made it crystal clear that cyber warfare is indeed a war. Therefore, it's advisable to hear what the experts have to say. Sun Tzu said that the victorious warriors first win and then they set out to the battlefield. The losers first engage in war and then think how to win it, (and I express no political view here). What's interesting in April's attacks is not the quantity but the attacked: NASA, the White House, and entertainment and defense companies. The types and goals of the attacks differed completely. Also the agencies attacked were diverse: civilian, governmental and even law enforcement agencies that are supposed to protect us. The world is changing. Applications like Twitter, Yahoo, Facebook can assist hackers in attacking us. Even the average bank robber gathers information before breaking in. he takes pictures, tries to understand how things work, he tries to put his hands on the bank's blueprint. Today, in the open source intelligence environment the bank employees are those who provide the intelligence. They believe that in Facebook it's only them and their friends and no one else watches. New Wi-Fi, LTE, Wimax technologies enable us to stay constantly online. The times when we used to stay online for five minutes lest someone would attack us are gone. Operating systems keep on changing as well. If once being a hacker was easy, it was as easy to secure information because there were

only Microsoft and UNIX and that's more or less all there was. Today we have IOS operating system, and we have hacked IOS; there are various Android versions, even HTML that once hardly managed to present any good pictures or text, nowadays it's HTML5 which enables us to do many interesting things. Therefore, the multitude of threats is hardly surprising. It's very difficult to protect systems and applications in a chaotic world. More than ninety percent of attacks are not carried out by official elements (although, supposedly there is some government agency planting "Flame" malware, and then everybody is talking about it). On the other hand, the government is becoming a preferred attack target. Around forty percent of attacked agencies are government or quazi-government agencies. If critical infrastructures like finance, telecom and such are also included, then they will total in more than half of the attacked targets. Also types of attacks vary. About half of the attacks are very simple. DDoS causes a small damage, but the other half are sophisticated, very threatening attacks.

The problem is above all regulatory. There are no regulations on IT intrusions; and reporting events is not mandatory. I welcome the initiative of the Israeli Cyber Initiative and the subsequent establishing of the INCB. The bureau was founded only in January 2012. Israel is very advanced compared to other countries regulation-wise. Yet, mandatory reporting is still not obligatory and many are unwilling to report. Therefore, we are unaware of some of the attacks in progress and we are aware of the existence of a threat. A newspaper reported on attack on a financial system. Two weeks later another report said some media websites were attacked. No one ask if the attack originated from the same source, if one attack was done for information gathering purposes or a pilot attack as preparation for the coming attack.

Focusing, investigating and understanding the source of the attacks as well as understanding the hacker are of vital importance. I've listened very carefully to NDS's Abe Peled's lecture, that beyond the great things he has done, he is responsible for constructing the first commercial internet website in Israel. Also, Elron's first internet provider is his work. If there was no internet in Israel, we wouldn't be here. I've listened with interest how NDS managed to eradicate piracy. They focused on the attacker, and I'd like to talk a little of the ways to deal with that hacker.

First of we ought to know his identify. He might be a soldier

of an enemy country, someone who wants to make money or someone whose self esteem is very important to him and he wants to brag before his friends that he can hack. If we learn who he is, we'll be able to guess why he is doing it. The person who hacked last time into Apple operating system- is an Apple employee today. So maybe it's a hacker who is hacking for a better job. Unfortunately, the majority of the hackers don't.

Secondly, it's good to know where the hacking is coming from. Is it from a civilized country where he can be dealt with legally and the police will charge him; or is he operating from a country that actually encourages him, hence he will have to be dealt with by other means. If we come to understand where he comes from, how he learned to become a hacker, we'll be able to guess which method he uses to hack us and what tools he is using; and then and only then, we'll be able to decide on our next step. Ultimately, since we are the victims we also want to know what to do. Multi-level-intelligence means information gathering. Big Data had been around for years, but it wasn't called Big Data then. Today, it's become bigger, today it's information gathering from multiple sensors and sources: internet, applications, firewall and sometimes also from open systems, Facebook and such. How can this information arriving from different sources be structures and processed for analysis? In order to be able to block an attack real-time, online and offline analysis should be done. Analysis is very important because in cyber world a lot of preparation work is done before the serious attacks are carried out. If we can identify the process of the information gathering, of attempts to find the open port, the problematic application, then we could prevent the attack. Only after the analysis, root cause analysis can be performed. Such advanced warning can prevent the great damage of the attack and even the attack itself. There is a moment in which we have to decide; and if we haven't decided it can be too late. Credit cards and state secrets can be hacked and the possibility that we have been attacked and we are unaware of that also exists.

We take the ample experience we have gained at NICE with Big Data, we analyze it, synchronize it with the intelligence of the cyber world and implement it on behavior analysis systems and intelligence analysis systems. We work closely with government and civilian actors. When we succeed in analyzing the information and provide the right people with the right information at the right moment, at that very moment, the crucial moment, those people will be able to take the right decision and protect themselves.

04

Fourth Session: threats and Challenges in the Cyber Dimension

New and Renewed Threats in the Mobile World

Mr. Adi Sharabani | CEO Skycure Security

When we talk about the threats organizations face in the mobile world, we are talking about new as well as the old threats we are familiar with, but they keep on changing in the mobile world and become much more acute. Threats can be divided into five main categories:

Physical loss or theft: very painful physical threats for individuals, and more so for organizations. Some hackers can gain total control in 11 seconds on a cellphone by connecting it to their computer. Its implication is that they have in their possession a real tracking and eavesdropping device for all intents and purposes. The device goes everywhere with its owner, meaning it can transmit the person's location to the hacker, hence the latter can listen to conversations, read private emails, learn about one's appointments etc. This presents a very serious problem for organizations. The majority of the existing solutions in this area focus on remote controlling the cellular device and deleting the stored data once it's stolen. But the more acute problem is identifying a theft or alternatively identifying the device that has been hacked.

Malicious applications: there is an exponential rise in the number of malicious applications. Many times, when we check malicious

applications closely, we'll discover that they reveal what they are doing. It's mainly valid for Android devices. For instance, there is an application that asks permission to access all data registered on a person's Android device, his location at any given time, detailed phone calls and such. Some people will not consent, but most do. It's by far more serious in organizations because they can't really trust their employees to make the right decision. Consequently, in the organization there are many employees infected with that type of malicious applications, which use the employee's mobile device accessing the organization's restricted resources. At present, the market has to offer solutions only for Android devices. There are no concrete solutions for Apple operating systems since Apple's "Walled Garden" model makes it very hard to develop technologies that solve those problems. These solutions rely mainly on identification of virus or of known malicious applications and their signatures in the users' devices. Meaning, it's a relatively old-fashioned model. There are many attempts to solve this problem in a generic way: to identify those malicious applications without having prior knowledge about the applications- but those attempts have yet to yield fruit.

Unsecured networks: it's about a network with one malicious user that can actually see all other users' activities. This problem is not only of malicious users, but also of users with malicious software. In that case, their device can also serve as remote attacker for launching an attack on all that network's users. The problem exists in encrypted networks as well. It's important to mention that the malicious factor can also plant Trojan Horses on the other users' devices, that link to the organization's network and can access restricted resources.

Breach in the device: bugs in the operating system or application might create a breach to be exploited by the attackers to gain control over the device. For instance, an attacker can take advantage of some vulnerability in Android devices to gain control of the user's device without the person's knowledge. This breach is very hard to solve since the majority of existing solutions rely on for the vendor's patching. Immediately after the notification of the security update, many attackers are trying to use those breaches in order to attack the users that haven't updated their devices yet. Nowadays, companies are trying to enforce software updates on their employees and verify their devices will always be updated.

The privacy issue is also included in this category. It's not about malicious applications trying to deliberately perform some

criminal activity, but applications that are supposedly innocent and they very well may be, but they breach users' privacy and furthermore the privacy of the business. Can organizations demand of their employees not to use a common application like LinkedIn that even serves those organizations for their businesses? My partner Yair Amit and I exposed in the New York Times that LinkedIn uses a mechanism that shows the user's appointment calendar within LinkedIn's application, instead of showing it only on the device. Behind the scenes for unclear reasons, LinkedIn decided to provide its servers with that info. This appointment info includes the organizer's name, his email address, topic, personal details about the meeting: communication details, phone number of conference call, conference call's password, the meeting's location, the people who will be present and so on. What is even more serious is that those applications send users' sensitive info to a third party or remote websites. And what makes the problem even more acute is that they do so without revealing that fact to their users. In the case of LinkedIn the problem is even more complicated, since there is no apparent reason why they had to send sensitive info like conference calls' password to the company's servers. We work in cooperation with LinkedIn for solving this problem ASAP. One of the most important things is that the fact certain applications access the users' personal details is often acceptable.

In conclusion: five main threats facing organizations that allow their employees to bring into the company private cellphones were discussed here. We ought to discuss the existing and non-existing solutions for each individual threat.

Constructive Ambiguity in Cyberspace: The Legal and Policy Challenges

Adv. Deborah Housen-Couriel | Yuval Ne'eman's Workshop
for Science, Technology and Security.

In this era the existing uncertainty regarding players' behavior in cyber space concerns everyone. Countries, organizations, companies and individuals are operating in a world which lacks clear, agreed upon, efficient political and legal regulation. Phenomena like Flame and Stuxnet accentuate the uncertainty and impotency of the international community. We are baffled, hesitant and also solutionless. It is known that cyber activity is harmful, yet we're unable to define the extent of the damage. It's hard to identify cyber attackers, and even if we do identify and catch them, it's more than likely we won't know what to do with them. Cyber-attacks present difficult questions to the international law and the decision makers. What can countries do and what is forbidden for them to do in cyberspace? How can we protect ourselves against virtual attacks while the identification of the attacker is uncertain? Is there a difference between activities whose results remain within the cyber space, in the virtual space to activities whose results are felt in the physical world? How to cope with the extensive economical implications of improper internet activity? Also in cases in which there is regulated behavior code on the international level, like the case of the European Council 2001 Internet Protection Act, enforcement challenges are still immense. Here we'll review some developments at the international level, will point out a central dilemma and will recommend two possible avenues of action in the global view in order to promote the educated development of binding legal norms and more transparent cyber policy.

My claim is that in spite of the efforts on the part of some of the international players, the uncertainty about what is allowed and what is forbidden on the cyber domain falls within the term "constructive ambiguity"- a term attributed to the former American Secretary of State Henry Kissinger. Kissinger applied the term of constructive ambiguity in sensitive diplomatic context in which the involved parties agreed upon letting the relationship between them be left without clear definition or final decision. An outstanding example is the Shanghai deal, in which the USA and the People's Republic of China decided to formalize of relationship between the two countries, leaving aside some unsolved issues like the sovereignty of Taiwan. Kissinger's solution was to leave the Taiwan issue as an issue within constructive ambiguity. In cyberspace we currently experience constructive ambiguity. In effect it was decided on the regulatory and legal level not to decide. On the one hand, countries and organizations recognize that it's a core issue that the international system must deal with. On the other hand, there is an unspoken international consensus right now not to regulate the activity in cyberspace. The common, accepted policy is that there is no need to rush towards binding regulation, treaties, memorandum nor code of behavior. That's because some of the main players regard such arrangement as limiting their freedom, and in addition the decision makers might be facing a complex dilemma. Yet, I claim that the present approach of constructive ambiguity is a mistake regarding the cyber domain. We can already see the serious results of the unwillingness to set clear and transparent norms that will enable close international cooperation in identifying attackers, a joint effort to develop the required technical means, a swift and efficient enforcement agency that sets a real preventive price tag to harmful activity in the internet and confronting the probably most difficult question - what is a harmful activity on the internet.

As to developments over the last decade of tendencies: many countries worldwide have declared publicly their transparent national cybernetic policy. Consequently, documentation about each country's view in respect of cyber space and the way it intends to act is accessible and known by other players. The ambiguity is lessened. Naturally, not everything is open, but a considerable part of the countries' views is there. By so doing, the decision makers have expressed publicly and formally the importance they attribute to managing cyber space. Interestingly enough, in many cases the people who signed on

the cyber policy document in leading countries like the USA, England and France, are the head of states. President Obama signed the policy document which testifies to the fact that the leadership attributes this issue the utmost importance. Although Israel has not yet declared publicly its general cyber policy, the National Cyber Bureau is working on it and already announced some elements that the future policy will include. Beyond the activity of specific countries, there is a collection of international initiatives held on level of international corporate organizations and collections of various states. The organizations are trying to increase certainty and transparency of cyber space behavior. Some obvious examples to the above mentioned activity include treaties, memoranda, joint cyber exercise and reports. For example: the European Council regulatory regime CHIPA, NATO's Tallin's Manual, aiming at setting international law norms relevant for cyber warfare; the international treaty draft presented by Russia and China to the Secretary General of the UN in September 2011 and also other relevant initiatives from OEDC, the EU, the ITU and international lawyers proposing drafts on cyber treaties.

Certain progress in attempts to develop specific enforcement measure to cyber in the Interpol, Europol and others is visible. A number of positive beginnings for forming international effective norms are at sight. The dilemma leading to constructive ambiguity in the cyber field is an ethical one stemming from the tension between two sets of values. On one side there are the values of the individual freedom of the and freedom of information including the freedom for information to cross political borders; on the other hand there are the values of info security, national security and the state's sovereignty, and the latter ones entail controlling, monitoring and intervention- all in contradiction with the first set of values. Penetrative actions like those of the hackers', crime organizations' make us more vulnerable than ever. And from that stems the main problem of leaving the existing situation of ambiguity in the cyber field as is. Since very little is known about what is allowed and to what extent in cyber space, a situation arises in which all actions performed in the cyber space in order to advance the interests of a country, organization and the individual can be used by others against them.

In conclusion, it's important to move forward on both levels. On the global level, in order to reduce the existing normative ambiguity and to advance to a situation of more certainty and

agreement on norms of operation, two things have to be done. Firstly, an international global forum with representatives from organizations, countries and individuals under the patronage of some international relevant organization like ITU or OEDC should be formed for the purpose of international focused cyber talks. It's vital to allow talks at global level, even if we learn that at present a close international treaty cannot be reached. Secondly, strategic thinking at the level of the new international order ought to be enforced. A dedicated international agency, similar to the WTO or the IATA, which will enable on-going professional dealing in issues relevant to global activity in the cyber space – is required. Eventually, reducing the constructive ambiguity in the cyber space depends on the willingness of the international players to commit to effective political juridical regulations.

The Cyber Threats on Developing National Defense systems

Mr. Doron Rotem, Director | Crisis & Emergency Solutions,
Israel Aerospace Industries.

The defense industries worldwide enter the cyber realm because it presents a business opportunity. On the other hand, they are also victims of cyber, since they constitute attractive and undoubtedly strategic targets for inflicting harm on their countries and security systems. We can safely say that the Israeli defense industry is a highly valuable target for cyber attacks and generally the prevailing trends and conditions today in the cyber industry tend to favour the attackers. There is an increase in the usage of organizations in external contractors and out sourcing as part of the global streamlining process and it's an overall trend: content, production and info systems. There is an increasing process of using computerized tools for planning, and a greater dependency on tools such as operating systems, info databases etc. Israel is in an even more difficult situation. We are a small country, hence it's impractical to rely solely on ourselves to develop all or even the majority of the required tools; and the question is how do we develop and maintain defense system in spite of all these threats. Let's take as an example the standard components in which "backdoors" are planted. It's discovered in missiles and all sort of defense systems when the aim is enabling remote disruption. Not everything has to be done in the development process. Every system has maintenance, spare parts. For instance, attacks are carried out by means of cards that were used as spare parts for Dell computers. We are talking about large, reliable companies from the defense sector with significant security, monitoring and advanced technology for these issues and yet they too fall victim to components that

some of them are simply commercially faked and some are planted into the systems: airplanes, battleships and missiles. Sometimes, even when things are discovered, the companies keep on buying from the same manufacturers.

Attacks on operating systems, organizational applications and networks were discussed here; but if we look at the hardware development process, it's a process of planning, defining needs and specifications. All done with computerized tools. That is to say, there are all sorts of applications for design, planning and verifying that run on the computers that are on the Internet. These are penetrable and it will suffice to change one line in the component specification of a, a circle on its silicon layer in order to alter its functioning. Is it avoidable? After all it's known that not all components are reliable. If so, in the framework of the organization they ought to be made reliable. For instance, there is a process of development to partially compatible components, of components that are exactly according to their specification, and components completely compatible to a specific system. In effect, a system manufacturer sometimes produces within the organization the specification and maybe part of the design, but many a time it's done by contractors, and the production itself is definitely done by contractors and the manufacturer receives the complete package. He knows to check whether it is right, but has no control over the process. There is not even a single stage in the process that is completely safe. We can get the impression that there is a certain division of the various types of attacks on a certain cross-section: at what stages the attack is carried out, the stages of development, technological layer, what is the trigger etc. What is interesting is the big variety. For instance, how is the component operated? There are components that initiate malicious action when they receive current in a circuit, but there are also others, more sophisticated that are being operated according to a certain timing, specific combination of logical events inside the circuit or something external like a certain input, a combination or input chains, temperature or all sort of external activities like inserting info via electromagnetic induction or inserting signals on power lines. This is only part of the attacks that can be carried on software.

As for software: there are two issues that don't receive the attention they deserve: maintenance and testing.

Every software and every system with software has a life expectancy. Even after having passed the development stage, after being checked and tested and found "clean" it's not

penetration-proof.

The second issue is the checks and tests. We must always assume that all prior steps we have taken failed and the components are unreliable. Therefore, at the testing stage, we'll try to discover that the system was compromised. But such tests never include all possible scenarios, it's always sampling according to some regularity. Tests are actually constructed according to specification, but cyber attack produces a threat that is not written in the Specification. Consequently, we can't know what test to design and it could prove to be a great challenge. For instance, how the same hardware components are accessed ? It can be done through power lines, to design them in a certain way and thus plant info the component that can receive unplanned input. Another example, an attack can be carried out by means of planting a component that eavesdrops to communication lines and actually to the encryption key and passes it onward. A planted component can also export info by modulating the power supply line.

Iron Dome is a good example. There are many ways to disrupt a strategic defense system and many ways to attack each individual element. Suppose the interceptor missile has a component that causes disruption only if the missile is on a specific trajectory and at certain altitude. Discovering such a component in tests is a significant challenge.

There are many types of hardware anti-tampering. If we look how an organization ought to get organized, the protection of the system by means of internal defense means ought to be in the core. But the second circle that includes the supply chain and contractors, and the third circle that includes the supporting system - teams that ought to be trained, research laboratories, regulations and such- all need to be protected as well. In MALAM of the Israeli Aerospace Industries all these aspects are being dealt with by means of training, solutions for early detection and cyber situation room for the company. We provide our solutions for other organizations. MALAM built the national situation room in Israel.

The Threats of the Age of Cyber-Warfare

Mr. Eugene Kaspersky | Chairman & CEO, Kaspersky Labs

Good evening ladies and gentlemen. I don't speak Hebrew. I just know some words. As I understood this is the last presentation today so I'll be as short as possible. So today I am going to speak about two main issues in IT security: cyber-crime and cyber weapons. How to make this digital world safer? First of all a question: how many people here in the audience really know how many computers they personally use? How many computers are installed in your car for example? Maybe in your kitchen? What about computers everywhere around us? Actually we don't know. There are so many that we really don't realize. Half of my life I spend in hotels so when people ask me: "Eugene where are you based in?" I say: "well, today in Sheraton but I pay taxation in Russia." So when I came to the elevator in my hotel and I pressed the bottom I understand there is a computer somewhere. It's not a hotel employee who makes a decision which elevator comes first, it's a computer, little computer somewhere. And it's everywhere around us and actually it's a completely digital world. If you pay attention, new railway systems in some countries have the trains report position and a computer decides the speed of the next train. The cars are getting more and more automatic, and I'm not talking Japan, where the navigation systems connected all the time and it's actually possible to manage the navigation systems from outside the car and it's everything, everywhere. Sometimes we really don't realize how deep we are in the digital technologies. How many of you still use paper, printed encyclopedias? I don't. How many people here? No one? And you are in a university. Well how many people don't use online

encyclopedias? I don't. How many people here? No one? And you are in a university. Well how many people don't use online encyclopedias like Wikipedia? Well, especially kids do. Kids are a completely different nation. There was a very good definition about kids. They are born in the time of internet, they are digital natives. We, adults, are digital immigrants. I still remember time without Internet. I do remember what a floppy disk is and still have an 8-inch one in my office. But the kids, well... It's the end of the day but I think it's good to wake up a little bit. I have a story for you about the little girl. The little girl was at home, she recognized a bird on a tree outside, she came to the window and genuinely tried to pinch-zoom the window! So when we are talking about the digital world we need to keep in mind that we are different: we are digital immigrants, kids are natives and the kids can't live without the digital technology. They can't realize the world without internet, without mobile phones. A friend of mine from Germany told me that his boy told him that he could live without electricity if there is still a battery in his computer. He will be OK with no electricity - but not without the Internet. All the entertainment, education, personal life, and social media is there. How many people in the room have more than five social networks accounts? So many, well if there were only one or two I would report your names to your boss. Because if you have five accounts, when do you have time to sleep? When I was a student I had to split my time between education and girls. Now it's more difficult - the kids have to split the time between girls, education and internet. So that's crazy.

But it's not just personal life. Businesses, industrial systems, everything is connected and depends on computer systems. Do you know a business that doesn't depend on computer systems? If you pay taxes, you have a computer to report your taxes, right? Computer-free business is only possible if you evade taxes. So it's everywhere - and it's under attack. The attackers 3 categories are cyber criminals, activists and cyber combatants. Not many people recognize activists as a threat, but actually activists do attack private companies, enterprises, governments, military resources. I'm afraid that activism is very dangerous, because in the future they can grow to become cyber terrorists. That's why I made a short comment about activism.

Cyber criminals are everywhere. It really is a global business. A couple of them are from Israel, also in a gang that did the largest bank heists. The 2005 attempt to hack the London branch of the Japanese Sumitomo bank to get 220 million British pounds,

fortunately was not successful. They successfully attacked the bank network, they got access to the critical bank resources, to the transaction servers - but they didn't fill the form in the right way. And that's what alerted and they were arrested. Good. Of course you know the case of Estonia. Estonians still think it's the Russian government behind the attack. I'm sure it was not Russian government because at that time Russian government wasn't so smart. So there were Russian spammers in the Russia undergrounds, Russian criminals who were coordinating the attack - and they crashed Estonia. This is very close to cyber terrorism and this is one of the cyber terrorism strategies, one of the scenarios which are coming to my mind - attacks on the internet infrastructure or maybe mobile networks. Cybercrime can do that. This of course is business because these guys are motivated by money. They earn a lot of money and sometimes they just behave like companies, like legal businesses. See the price list for botnets, and even the ICQ number for the technical support calls, terms of service. Some of the cyber criminals even have press releases, blogs, and forums. Russian cybercriminal gangs had partner conferences, so it's not just a little criminal behind his computer somewhere. It's an organized business, the only difference being that they don't pay taxes. It's organized but not the same way as mafia. It's not like a godfather, family, soldiers and management. It's like independent businesses and individuals which trade information among them. Unfortunately it's a very profitable international business for them. 19 year old guys in a new BMW 7 in Moscow. How many people in the room have a BMW 7? I'm not trying promote cybercrime -but it's easy, the only things they need are the computer plus internet connection and some knowledge. Unfortunately there still is a lack of cooperation between police departments from different countries but finally governments recognized that this is a very serious issue so they need to cooperate. I was talking about internet Interpol for maybe ten years. Now Interpol finally announced opening their cyber division in Singapore. How much do we lose from cybercrime? A couple of years ago we tried to calculate the damage to the global economy from different types of cybercrime. This is only malware based cybercrime, not about credit cards and other types of cybercrime like illegal hosting and etc. Just the malware based cybercrime, we estimated costs at least \$100 billion a year. McAfee made a similar survey but in a different methodology. They interviewed companies, and their result was \$1 trillion a year. The global damage of malware based

cybercrime could be from \$100 billion to \$1 trillion. Compare it to the damage from the recent Japanese earthquake and Tsunami which was around \$300 billion. In the Internet every year we have 1 to 3 tsunamis and earthquakes. We don't recognize it really because the victims don't report in many cases and sometimes individuals don't report to the police. It's like radiation. It's really bad but in most cases we just don't recognize it. It is very bad but unfortunately it can be worse. The catastrophes: do you remember the 2003 US blackout? The cause probably was that squirrels cut the links. So, squirrels in the US also connect to the internet. There was a cascade squirrel attack. Of course not. There were more realistic reports about the malware, on the same day there was the Blaster attack. I think many people in this room still remember that day in August 2003 when Blaster infected and crashed Windows and Unix machines. Actually they were not crashed but frozen, so the UNIX machines were looking like working but actually they were out of service. The 2008 Spainair plane crash. That was first of all a technical mistake, second the human factor and infection. The reason for the crash was the fact that a plane had technical faults. These problems in the plane were not recognized on the ground by engineers in the ground checks, because their computers were infected and engineers didn't have access to the database so they couldn't properly understand the diagnostic. It wasn't translated to human language. The virus wasn't the reason for the catastrophe, but it could have not happen without the virus. I'm sorry, but maybe some people here are not happy with what I'm doing with Stuxnet, Duqu and Flame research. I'm really sorry - but it's nothing personal, it's my job. Stuxnet infected so many computers around the globe and that was really dangerous not just for the countries that are in this game but also many other countries around. So next time, please, be more accurate! Ok so it's my question today – will it happen again? “Ken”.¹ Because still the machines have so many faults. Just a couple of examples: a report for 2007 demonstrated the plane avionics network was connected to the passenger network. A firewall was there, but so did vulnerability so passengers could access to the navigation systems, flight control from the passenger seat. Keep in mind that these planes are also connected to the Internet now, so a ground based hacker could access the flight control systems. Why don't you smile? Of course you know about an American drone that was intercepted and landed in the country I can't mention here. It's not just me talking about

how serious the future cyber-attacks could be but also the top government officials. Unfortunately it's possible to hack anything. I just want to quote Leon Panetta, US Secretary of defense, that in case of a successful cyber-attack it could paralyze the United States. Exactly the same is true for any country. That's why cyber weapons are a very bad idea. First of all, it's easier and cheaper to attack contrary than with traditional weapons. Second, cyber weapon can replicate unlike traditional weapon and cause collateral victims. The rest of the countries will learn that and actually I'm afraid that in the future there will be other powers in this game because it's just software, just knowledge. The countries that don't have enough expertise, countries that don't have the engineers will employ them, or maybe kidnap, or maybe activists will grow to the level of terrorists and maybe traditional terrorists will be in touch with cyber terrorists. These ideas are spreading fast and this is a genie in a bottle. I'm afraid that if we don't stop it now, this genie will cause much more problems. So my message is: stop doing that before it's too late! Unfortunately it is very difficult to protect against cyber weapon. The only way to protect is to redesign the industrial systems, to rebuild all these SCADA systems on a secured operating system. So we need to replace Windows or Linux systems with a secured operation system and redesign old SCADA software. Actually we have a secured operating system but I'm not going to sell it to you today. We have a secured operating system so I know what I am talking about and this is the right way to protect the systems but until we have it, it will be quite a lot of years so the only way to make this world more safe and secure, how to protect your country as well. There are a lot of software engineers in Israel, I know. But not enough to do that in say 2, 3 years. Maybe 5 years. So for the next 10, 15 maybe 20 years many critical systems will be not protected, and I'm afraid that this cyber boomerang might get back to you. I'm really scared about these scenarios. Internet doesn't have borders. The systems are very similar. I'm afraid that we will have more and more Stuxnet scenarios in the future and I'm afraid victims will be in very different countries.

So how to make this world safer? I think there are just three major ways. Actually we have technologies, national regulations and finally international treaties like United Nations and Interpol taking care about cybercrime so I'm pretty sure the population of cybercrime will be under control. But I still see that most of the governments recognize cyber weapons and cyber sabotage

as an opportunity. I recognize it as a danger. I don't know who is I right - the future will tell. But I have a nightmare that a well designed cyber-attack will get us to the pre-electric age. Horses, candles, hand written paper mails. I think it's a place for international cooperation, international treaties, maybe United Nations to get governments to the same table and to agree that cyber weapon is forbidden. Not to use, not to distribute, not to teach bad guys - and that is the right way to make this world, and your country, more safe and secure. Thank you very much.

05

Closing session

Rabbi Prof. Daniel Hershkowitz, Israel's Minister of Science and Technology

Cyber is a domain that occupies almost everything in our lives. The development of the computers is probably the biggest revolution of the twentieth century, since it led to an enormous development of sciences into unexpected directions and brought about the development in communication and databases fields. Today, unlike in the past, internet provides instant information; via search engines it's possible to instantly discover whether relevant keywords are included. These things created a revolution that impacted the scientific development. Among other things they brought about the development of the Interdisciplinary studies, which at present are the most sought after course of studies in science. Science occupies a major part of our lives, a part that brought with it endless possibilities. Actually, the sky is the limit, because the world has become ever so small and accessible that almost everything can be done from almost everywhere. However, with the great possibilities arrive, of course, the risks, but all in all a huge window was opened for the state of Israel. Although Israel is not among the big countries terrain-wise, population-wise or natural resources-wise, we are blessed with one immense treasure: our human capital, that in many aspects compensate for the lacks in the material. Israel has become a science and technology superpower. One of the prominent people behind this conference, Prof. Ben Israel, chairs among other things the National Council for Research and Development

and the Israeli Space Agency. The tiny state of Israel is in effect a space superpower that even a giant superpower like the USA is courting after, because Israel has space technologies that the USA needs: lightweight observation satellites, hyper spectral satellites, SAR satellites and such. Israel has become a science and technology superpower thanks to the special human capital, the very same that stands behind the cyber domain. A special window of opportunities has opened for Israel in which cyber has become more dominant in international relation, both at times of peace and times of war. Since today threats are coming from all directions the damages of cyber attacks can be tenfold higher than those of a war conducted with conventional or unconventional weapons. This window of opportunities brings about one of Israel's great advantages - thinking "outside the box". This characteristic and not knowledge or education is the one which makes the difference between good and excellent. Sometimes, a negative correlation exists between thinking outside the box and good educational system, because the latter one, by definition, teaches to think within the box. Therefore, one of the things that characterize the Israeli scientists is thinking outside the box that in my opinion constitutes one of the more dominant tools in developing cyber capabilities. That's why it was only natural to receive a directive from the PM to place Israel among the first five leading nations in the world in the cyber field. It's not presumptuous for a country like Israel. The Ministry of Science and Technology and Prof. Ben Israel as the chair of the National Council for Research and Development led a joint project of over seventy experts from various fields in order to prepare the infrastructure for the National Cyber Bureau. As I have already said the possibilities are endless, the sky is the limit and I wish us all that we'll use those tools correctly for peaceful and developmental purposes.

Mr. Benjamin Netanyahu, Prime Minister of the State of Israel

I'd like to welcome all the people present in this conference and wish you all enriching discussion. We are dealing with a very important domain- the cyber domain – which became fascinating and of utmost importance economically, defense-wise and academically. That's why a National Cyber Bureau has been decided upon and it'll integrate those three fields. First, for the defense on the state of Israel. Every country today is exposed

to attacks on its computerized systems, the infrastructure system, communication and others. Each country has to build its defense tools and Israeli will certainly keep on doing that. Cyber domain also presents an opportunity to develop entire industries worldwide. Israel is blessed with many such companies, and the government is interested in developing and reaching that target jointly with the security agencies and the academy, and academy includes universities as well as schools. We aim at integrating the three fields in order to turn Israel into a prominent force, even a cyber-superpower. This entails a huge investment: it entails for us to always be at the forefront of development and innovativeness. In order to be considered as a cyber superpower, a country doesn't necessarily have to be large, but blessed with knowledge and talents; it has to be a brain superpower. I think Israel has that in abundance, hence the target is for Israel to be among the leading superpowers in cyber, and I am positive the target will be achieved, among other things thanks to conferences like the Yuval Ne'eman Workshop for Science, Technology and Security holds.

**Yuval Ne`eman Workshop
and the National Cyber
Bureau`s 3rd Annual
International Cyber Security
Conference – Creating
Cyber Ecosystems – 2013**



Yuval Ne'eman Workshop
for Science, Technology and Security



Prime Minister's Office
National Cyber Bureau

You are cordially invited to attend the Yuval Ne'eman Workshop
and the National Cyber Bureau's 3rd Annual International Cyber
Security Conference

Creating Cyber Ecosystems

Wednesday, June 12th 2013, 07:00-18:30, Smolarz Auditorium,
Tel-Aviv University

Program:

07:00-08:30 **Reception & Registration**

08:30-10:00 **Opening Session - Policy Makers**

Chairman: Prof. Maj. Gen. (Res.) Isaac Ben Israel, Head of the
Yuval Ne'eman Workshop for Science, Technology and Security,
Tel-Aviv University

Greetings: Prof. Joseph Klafter, President of Tel-Aviv University

Dr. Eviatar Matania, Head of the National Cyber Bureau,
Prime Minister's Office

Mr. Avi Hasson, Israel's Chief Scientist

His Excellency Shimon Peres, President of the State of Israel

10:00-10:15 **Break**

10:15-12:00 **Short introduction of the Yuval Ne'eman Workshop Cyber Activities**

Mrs. Gili Drob - Heistein, Executive Director and **Mr. Ram Levi**,
Senior Researcher, The Yuval Ne'eman Workshop for Science
Technology and Security

First Session: Cyber Readiness and Technology

Chairman: RADM Ophir Shoham, Director of Defense R&D

Ms. Melissa Hathaway, President, Hathaway Global Strategies, LLC,
Former senior director for cyberspace at the National Security
Council, USA

Cyber Readiness: Is Any Nation Prepared?

Mr. Art Coviello, Executive Vice President, EMC, Executive Chairman,
RSA

Intelligence-Driven Security: A New Model using Big Data

Mr. Paul de Souza, Founder & President, Cyber Security Forum
Initiative (CSFI)

Building Cyber Warriors

Mr. Robert Shaw, CEO and President, Net Optics, Inc.

Leveraging SDN for Network Visibility, Security and Threat Response

Mr. Adi Sharabani, CEO, Skycure Security

Wifigate - How Carriers Expose Us to Wifi Attacks

12:00-12:45 Lunch Break

12:45-14:15 Second Session: Cyber War & Peace

Chairman: Erez Kreiner, CEO, Cyber-Rider Ltd.

Mr. Richard A. Clarke, President, Good Harbor Security Risk Management, Former Special Advisor for Cyber Security to the President of the USA

[Cyber War, Cyber Peace](#)

Dr. Thomas Rid, Reader in War Studies, King's College London

[The Attribution Problem - A Fresh View](#)

Mr. Ilias Chantzios, Senior Director, Symantec Government Affairs-EMEA and APJ

[Building an Effective National Cyber Defense – Capabilities, Strategies, Policies](#)

Mr. Doron Rotem, Director, Crisis & Emergency Management Solutions, MLM Division, Systems Missiles & Space Group, Israel Aerospace Industries Ltd.

[System Approach to Cyber Research](#)

Mr. Eric M. Hutchins, Fellow and the Chief Intelligence Analyst, Lockheed Martin (LM-CIRT)

[Cyber Kill Chain™: Applying Intelligence to Defeat Cyber Threats](#)

14:15-16:00 Third Session: Cyber Technology: The Next Generation

Chairman: Gadi Tirosh, General Partner, JVP

Lim Chuan Poh, Chairman, National Infocomm Security Committee (NISC) and Chairman, Agency for Science, Technology and Research (A*STAR), Singapore

[Singapore's Approach to Cyber Security](#)

Panel:

Mr. Eli Yitzhaki, Strategic & Business Development Leader, ELTA SIGINT EW & Communication Division

Mr. Avi Chesla, Chief Technology Officer, Radware

Mr. Tal Mozes, Hacktics Leader, Advisory Services, Ernst & Young

BG (Ret.) Yair Cohen, Head of Cyber Security, Elbit Systems

Mr. Andrey Dulkan, Director of Cyber Innovation, Cyber-Ark

16:00-16:15 Break

16:15-17:15 Fourth Session: Hacking the Human Brain

Chairman: Prof. Nathan Intrator, Blavatnik School of Computer Science, Sagol School of Neuroscience

Dr. Moran Cerf, Neuroscientist, UCLA and NYU and ex-security expert

[Brainhack: How neuroscience can inform hacking and vice-versa](#)

Mr. Yanki Margalit, Social entrepreneur, Chairman SpaceIL, Partner Innodo Ventures

[Towards HOMO SAPIENS 2.0](#)

Dr. Roey Tzezana, Unit for Technology & Society Foresight at Tel Aviv University

[The Bare Minimum: Emulating the Brain in a Computer](#)

Opening Session - Policy Makers

Prof. Maj. Gen. (Res.) Isaac Ben Israel, Head of the Yuval Ne'eman Workshop for Science, Technology and Security, Tel-Aviv University

The Yuval Ne'eman Workshop was founded 11 years ago, and this is its 86th conference. The workshop focuses on cyber and space and in these fields we've been able to promote general interest in the state of Israel as is clearly reflected, among others things, in this conference. The Israeli National Cyber Bureau, headed by Dr. Eviatar Matania, is driving the campaign to increase national awareness to cyber threats, establishing a national industrial infrastructure in this field and promoting cyber research in the country. Academic research is a unique element in this campaign and we, Tel-Aviv University, are aiming to be in the center of this initiative, not only in Israel but globally.

Prof. Joseph Klafter, President of Tel-Aviv University

We are already amidst cyber warfare. The United States is tracking individuals suspected of terrorist activities by monitoring social media; China is accused of stealing advanced weaponry system designs from the United States; Iran is developing superpower scale cyber skills, attacking oil companies in the Persian Gulf and threatening the American banking systems. These are all the headlines of just the last few weeks. Technology is evolving, changing the world and raising new challenges. Thousands of

new security breaches are discovered each year in operating systems, infrastructure software, and especially in the field of applications. Security patches cover a mere half of these vulnerabilities rendering a prosperous civilian security market valued at around one hundred billion dollars. And so, without the whistles of shells and rockets, we are in the midst of the first cyber war in history, where the battles are waged with the arsenal of worms, viruses, and Trojan horses.

The state of Israel faces the opportunity of becoming a cyber-superpower. It possesses a rare combination of skills, an entrepreneurial culture, a venture capital industry infrastructure and a defense organization sprouting technologies and incubating innovations. To fully utilize this potential, Israel must act with a wide perspective. The cyber world is multi-dimensional, multi-disciplinary, and inter-disciplinary spanning across technology, engineering and computer sciences, social aspects, administrative aspects, economic, and legal aspects. With such high level of complexity, all eyes turn to academia. And here, in Tel-Aviv University, we've accumulated, along the years, the experience and reputation of formulating plans and multi-disciplinary content. Therefore, starting from the coming school-year, Tel-Aviv University has decided to establish a multi-disciplinary unit for the study of Cyber Security which will be offered as a part of the undergraduate curriculum for the humanities, social sciences, law, computer science, and engineering faculties. Students from the fields of humanities, social sciences, and law will also be exposed to the technical aspects of this field, including computer work, network protocols, and encryption. That way, a jurist practicing cyber law will also have the background in technological aspects of this field. Similarly, a student of the exact sciences will be familiar with the history of cyber culture, administrative aspects, economical factors, and issues of privacy in the digital world. In addition, there will be a year-long cyber workshop, which will cover a variety of topics in depth. Upon the launch of this new program, Tel-Aviv University stands in the fore-front of academic enterprise in the field of cyber. We congratulate those who are engaged in this effort and we welcome the new generation of students destined to lead the world of cyber.

**Dr. Eviatar Matania,
Head of the National Cyber Bureau, Prime
Minister's Office**

It was two years ago, in the first international cyber conference of the Yuval Ne'eman Workshop in Tel-Aviv University that the Prime Minister of Israel shared the vision of Israel in cyberspace. His speech here, along with government's Decision #3611 dated August 2011 were the pinnacle of the State of Israel's first official move into cyberspace. It all started in the early 90s with the launch of many high-tech companies in the field in Information Security and later in Cyber Security. This move was then followed in the establishment of the e-government services, known then as "Available Government," in the late 90s, and the establishment of the National Informational Security Authority in 2002. In 2010, Professor Ben Israel led the national cyber initiative, designed to explore the state of Israel's advancement into cyberspace, which culminated in the Prime Minister's speech here and the government's resolution in 2011, and the forming of the Israeli National Cyber Bureau, which officially began operating in 2012. One year ago, at the 2nd National Cyber Conference here, I outlined the two primary paths in which Israel is about to operate in order to fulfill the vision of entering cyberspace. The first path to take is the establishment of a comprehensive national defense strategy. It should include: national preparedness strategy, regulatory layers of defense, licensing, standardization and partnering with companies and different sectors of the population. On top of that, there will be a national CERT team which will cooperate with the various sectors in the economy, promote knowledge sharing initiatives between local organizations, and knowledge sharing with different sectors globally. We've already established a situation room operating 24/7, which produces a national situation report.

We refer to the second path as the as "building of the technological infrastructure." We believe that in order for Israel to remain a leading country, we have to work in parallel on these two routes of strategy and preparedness on one hand and the building of technologies and human capital on the other. This should include state-wide infrastructure, academic infrastructure, promotion of the industry as much as possible, the building of new start-up companies, and the establishment of research and development centers in multi-national companies. However, these tasks cannot advance without the nurturing of

quality human capital entering the world of cyber. In the past eighteen months that have passed since the establishment of the bureau, all government offices have been partners in this effort as the significance of cyber is paramount to all for the financial growth of Israel as well as its contribution to national security and building a defense perimeter for the country.

Where do we go from here and what is our vision of these two routes that I've discussed? This week, the Prime Minister and Minister of Economy launched the cyber week here in a conference that brought together technological start-up companies with investors. This signifies one of the primary targets that the government is trying to promote and that is finding breakthrough technologies in the world of cyber. The Prime Minister and Minister of Economy discussed Israel's status as a minor technological superpower. We view Israel as a global cyber incubator because the start-up nation culture is not restricted to technological entrepreneurship but it is also the willingness to adopt new things, the willingness to discard that that does not succeed, the willingness to experiment, the willingness to err, and to know that when you attempt to breakthrough and innovate you occasionally make mistakes. The willingness to combine things, to combine strategy and technology, will enable an eco-system found only in Israel. Israel owes its superior starting point in this field to its culture of entrepreneurship, its world-leading academic research infrastructure in the fields of computer science and electronic engineering, its technological infrastructures, its many technological companies, and its prestigious defense system. Israel, the global cyber incubator, is where our allies and friends from around the world will cooperate with us in creating a safe cyberspace as a place for global growth.

We extend an invitation to our friends and partners in this grueling journey, one that will take time, but will allow us to build state infrastructures and offer an opportunity to those who join to experiment in the process and study the technologies. All, of course, under a clear framework of how these things are done in international collaborations. Following intensive preparatory work, along with the Planning and Budgeting Committee and Ministry of Science and Technology, we will shortly announce the establishment of several academic research centers that will open in the coming three years, focusing on the technological world, the non-technical inter-disciplinary world (studying of cyber from psychological, moral, ethical, educational,

philosophical, and political perspectives), and also simulation research centers. We invite our friends worldwide be partners in these efforts and we have already seen positive responses.

Other partners have also shown interest in the industrial aspects of cyber, wishing to learn from our experience of promoting technological industries. In cooperation with the Ministry of Commerce, we are now building an extensive platform for promoting Israel's industry, ranging from using the Chief Scientist Office programs such as KIDMA (Hebrew for progress), which was announced half a year ago, as well as other elements that assure the governments support in the industry's development. These tools that will be used to promote the industry in Israel can serve as inspiration for others; we are not reluctant to share our knowledge and experience and lead the way in these fields. Another field in which our partners seek our advice in is the promotion of human capital. We are happy to share all that we can, which is the majority. We are currently planning a pilot for a virtual cyber school, Cycademy, which will basically allow for the training of students, teachers, professors, in Hebrew. Its launch can serve as an example for other countries to follow.

Cyber strategies are a topic of much debate in the world. Building cyber strategies and preparing for cyber-attacks is a difficult challenge, one that requires the cooperation of other countries through consultations with them. In these topics, as well, we look at ourselves as an incubator and the academic centers that I mentioned earlier will form another dimension in the research of these topics and the ability to share knowledge in Israel and globally. Being a global cyber incubator is important for the positioning of Israel in the world. Cyber is a global growth space, infrastructures are global, the threats landscape is similar, the world wants to build a resilient space, and we are a part of this world. Alongside building technologies and unique solutions for our country, because every country has to be able to protect itself, we also see ourselves as a part of the global world and here Israel can benefit the world. The route of building cyber strategy and preparation alongside the building of infrastructure, technologies and the building of an incubator ecosystem that is both Israeli and global, is the combination that will help us turn Israel into a global cyber incubator.

Mr. Avi Hasson, Israel's Chief Scientist

The title of the conference, Cyber Eco-System, accurately depicts its topic. We all deal with challenges, but the opportunity is nothing less than great for the state of Israel. When it comes to innovation, science, and technology, Israel truly is a minor superpower, standing in the forefront thanks to a unique combination of great science and entrepreneurial spirit, a combination that created the high-tech bio-technology, and medical device industries. Just this week, we heard about the sale of an Israeli technological company to Google for over a billion dollars. The world of technology is essential to the Israeli economy. In the field of cyber, even though the national project is new, our activity is not. In this field there is a sound foundation that can be leveraged. Some 200 companies (from very early stages to multi-national companies with world class innovation centers) operate in Israel.

In the Chief Scientist Office programs, we've processed, funded, and advanced this field in the academia, as well as in cooperation between the industry and academia, and in the consortium and MAGNET programs. Joint programs for the Ministry of Economy and the Administration for the Development of Weapons and Technological Infrastructure in the Ministry of Defense focus on dual research and development for security and commerce. The KIDMA program focuses on the field of cyber with a series of perks and benefits, and in the few months since the launch of the program grants have already been awarded to dozens of companies.

Academia is an important source for innovation, but future industries are both research intensive and rich in knowledge and we are investing in building an infrastructure in order to translate academic assets into commercial products in technological companies.

The vision of a global cyber incubator is aided by venture capital investors and the Chief Scientist incubator programs. We have the opportunity to position Israel in the lead, but the road is a long one.

International cooperation is at the core of the research and development and business activities. At the Chief Scientist's Office we allocate over 20% of the bureau's budget to this effort. Every year we match and fund hundreds of projects between Israeli and foreign companies, in 50 different developed and developing countries, in many fields including cyber.

The multi-national companies are important partners in

promoting the products of smaller companies as they offer the opportunity to launch the technologies incubated in Israel into the global market. It is equally important to open up to the world while addressing the challenges of clearance and secrecy. I emphasize that national resilience and economic security are main pillars in national security and that free trade and free export aren't contradictory to national security, rather they contribute to it. Balanced export policies must be established and set so as not to conflict with our fundamental interests, but at the same time the export policy must enable companies and investors to see concrete opportunity and bring these opportunities to actualization. It's important that the established policy and regulation does not stifle the initiatives and will be balanced by the national security needs on the one hand and the needs of the industry on the other.

His Excellency Shimon Peres, President of the State of Israel

Cybernetics is not merely a technological means, nor is it merely a means of warfare. As we discussing the danger of war, warfare itself is changing its face. In the midst of all the strategic discussions, unexpected fate changing interventions affect nations and their future. The recent two changes being, Unmanned Aerial Vehicles and cybernetics. As for UAVs, we are now discovering the potential they have in improving our lives, but also where they could be problematic. Much like in cybernetics, we may end up in a situation where UAVs are launched without us being able to ascertain their origin, destination, or being able to scramble our defenses.

Battling sides in warfare used to carry uniforms, flag, follow rules, and maintain fronts; they are perishing. The same can't be said for cybernetics. We have to find a means of protecting ourselves in the face of these emerging risks. For Israel, this is a risk as well as an opportunity. It is a great risk because we inhabit a country that has limited physical resources and it's a great opportunity because we're a country that has many human capabilities. Israel is an island in the global community; we are a lone people with no brother in language, no brother in knowledge, and no brother in history. We find ourselves trapped in general mayhem, not only about the essence of this war but also regarding the nature of this peace. The current events in the Middle East undermine the very foundation of what a state

is. There is virtually no one country that is unified in whole. In the past, our neighboring countries attempted to overpower us using their armed forces. Seven wars later, I think they've been discouraged. The crucial point in this process was the 1973 (Yom Kipper) War. The Arab armies, at their peak, took us by complete surprise and breached our defense lines, but ultimately, this great triumph turned out to be a near utter catastrophe. I think that it was after this war that they realized that they cannot overpower us in warfare, along with their suspicion of Israel possessing a nuclear option.

Some of our neighbors realized that they can't use traditional army tactics, so, in order to defeat Israel they switched to terror. The path of terror does not offer complete victories, only many losses. But at the same time, there's no risk of a great downfall because it doesn't matter how many terrorists you kill, there will always be others to replace them. The path of terror does not require masses of people: 15 men can reach Manhattan and take 3,000 American lives. The United States has spent one trillion dollars in the past decade unsuccessfully fighting terror. The Arab terror, in part aimed against Israel, is now harming the very same countries from which it originates. No force today has a more negative effect on the crumbling Arab world more than terror. In Gaza alone, there are five different terrorist organizations, all working independently. Gaza is consumed by terrorist organizations and so are Lebanon, Syria, and Iraq. And we, of course, must be careful and they should be careful because no one can be held accountable.

Cybernetics will not only drive technology forward but will also encourage other scientific alternatives. I don't view cybernetics solely as means of doing warfare, but I see cybernetics as something that will completely change the face of warfare. As time progresses, we will discover different types of computers, biological ones, method we do not yet know about; this is because strengthening our existing computers or protecting them will not suffice. We will also need to build computers that current cybernetics does not control. This requires tremendous great mobilization of our forces, not just technologically or militarily, but a complete and comprehensive recruitment of our resources. This starts from educations, the number of engineers we have, goes through intelligence and through statesmanship. You are poorly mistaken if you think you can triumph using weapons alone. Weapons can inflict loses upon your enemy, but I doubt if weapons can be the tools of peace. In addition

to weapons, we must have political wisdom and much like the weapons, political wisdom is not simplistic. Both have two sides. Without its advantages, Israel will be boycotted. Israel's fortune is that it is scientifically stronger than it is politically. Politically, we are 1 of 200 members of the United Nations. Scientifically, we're in the top 10 or even top 5 of nations. It's not just about getting a good grade, but it's more of a ticket to enter modern society in the same way that our political weakness isolates us. Across the border, I can see in Iran and Syria the sharpening of cyber knives. Others will soon follow. We must never cease striving towards being a leading force. Any scientific or military weakness will immediately summon attempts to harm us. This is why we have to preserve our qualitative advantage as quantity in itself slowly becomes insignificant. Let's say one nation has thirty nuclear bombs, they can pulverize their enemy thirty times, whereas another nation has a mere ten bombs; we all know that it's enough to annihilate once, you don't need the other twenty. So, the advantage comes down to quality, sophistication, something extra. We, the Jewish people, have a legacy that is sometimes hard and other times great. When outsiders ask me what is the Jewish people's greatest contribution to the world, my reply is: perpetual discontent. We're never satisfied; we always think there's room for improvement. If a Jewish person begins to feel satisfied, I begin to doubt his Jewishness. Satisfaction is for the lazy, the unmotivated. He who isn't satisfied seeks, creates, invents.

Filling the shortage of experts in this field is a vital effort in the current battle for achieving cybernetic skills. In my personal opinion, we must subsidize companies that work in this field. Criticism of such subsidy is wrong; if we don't subsidize, people will not take money out of their own pockets to invest in research. Even America subsidizes. We had a challenge with the electric car, the United States invested in three electric car manufacturers, each one for half a billion dollars. Two of those went bankrupt and the third continues operating thanks to subsidy. We need to support private business ventures as they are a part of our national effort. The vast majority of scientific effort is not being done by the government, so we must cherish and value entrepreneurs and inventors. The IDF is also fulfilling a huge role in scientific development. We are in the midst of a campaign, not behind it; a campaign whose full scale is not apparent, it is changing the face of the world and the face of peace because countries are now changing. Peace used to be

made between states whereas nowadays, the issue of peace is internal. Luckily, for us in Israel, in our internal disputes, weapons are not being used. Where there is no democracy and conflicts are resolved using daggers and bombs- it destroys the people. The economy is global but there is no global government; and so it effects each government but no government affects it. Terror is global and savage, it can endanger any person and any place and not even with our full cooperation will we be able to uproot it. We must be bold and audacious and focused on investing in being the first to succeed.

There is an ongoing discussion today around the future revenues from the recent discoveries of the gas fields. If we do have gas, let's invest it in the most promising thing, which is our children's education. Twenty-five years from now energy resources will change; we already see the growth of solar energy. Let's invest in our children, our youth, science; we must increase the investment even at the risk of inflation as there is no task that is more true, vital, and urgent than that of the investment in education, knowledge, and science.

Once properly organized, we can gallop forward in three efforts. Firstly, the face of warfare has already changed and is constantly evolving in the midst of the campaign. I mentioned, the UAVs and cybernetics, but there are other things as well. We can't afford to pause and rest and we must never be content. Secondly, alongside the technological advancement we must also promote political wisdom. Wherever we can stand down, wherever there is a bridge to be built or an opportunity for dialogue, we must try. Thirdly, invest in our children without delay. This is why I came here today, to congratulate this conference, and emphasize its essence and its profound vitality as we are in the process of deep and amazing changes, which we must deal with and cope with, provided that we see them in their full scape, in the magnitude of their severity, in their great depth, and that we put forth our best efforts. My best wishes.

01

First Session: Cyber Readiness and Technology

Cyber Readiness: Is Any Nation Prepared?

Ms. Melissa Hathaway | President, Hathaway Global Strategies, LLC, Former Senior Director for Cyberspace at the National Security Council, USA

One of my longtime mentors, Andy Marshal, who is the director of Net Assessment office in the United States DoD and has advised every Secretary of Defense since 1972, says that you need to look to your past to inform your future. Therefore I will start with a brief history lesson before I go into some of the current challenges.

The first message on the Internet was an exchange of email between two universities on October 29, 1969 and today we have more than two hundred million emails that are sent per minute. In 1972 the very first attachment was sent with an email, it was file sharing between the United States and Europe. Today the amount of data that is generated in a day could fill up football fields or soccer fields of information. In 1979 the very first automated cellular telephone network was created by Nippon telephone telegraph in Japan. Today mobile devices have penetrated more than thirty five percent of the population and there are more mobile phones than individuals on earth, also joined by plenty of IP devices. The domain name system was created in 1983 to enable the global expansion of the Internet and in 1985 the top-level domains were created.

Originally, the innovators of the Internet they had only allocated fifteen percent of the address base per dot com, which is part of the reason for the needed move from IPV 4 to IPV 6. In 1992 the very first instant messaging developed, it was tested on a 2-G network in Finland, laying a cornerstone for today's generation of revenue of more than eight hundred thousand dollars per minute. The ITU branded the interoperable standard for voice over Internet protocol in 1986. This invention gave way to more than voice over Internet - video over internet protocol and the like, which in turn allowed for creation of Skype in Estonia in 2003. Today many are listening to music or watching videos, viewing photos, extending tweets and all of that was enabled through that ITU interoperable standard for VOIP.

Finally, social networking technology merged in 2002 with the emergence of Friendster, then replaced by LinkedIn and the like. Now that twenty percent of the global population is using that social network, it is really changing the way we live, work and play. With these innovations, the attack surface is great and the exploitation is even greater. Today, within one minute there are more than a hundred and thirty five botnet infections and twenty new identity theft victims.

A decade from now there will be eight billion people in contrast to today's seven. Close to sixty percent of the population will use Internet-enabled devices, in contrast to today's thirty-five percent. IP-enabled devices will surge into homes and businesses and there will be closer to 10 such devices per person in contrast to the average of six there are today. Today we see this ICT innovation contributing to about four percent of our GDP in developed nations and tomorrow we're expecting the number to be as high as ten percent, because government and industry leaders believe and are adopting that ICT that's driving change.

In the old days there were mainframes, arguably, there are main frames again today -they are called cloud. We went from this to the desktop PC and now the mobile and each of those innovations have allowed for productivity gains and efficiency gains among our countries. The Internet is increasingly embedded into every part of our life, whether it is the new buildings that have the IP-enabled devices or the energy with control systems that are actually accessed through the Internet.

The new industrial control systems and manufacturing capabilities are being generated through the Internet and the Internet devices. In fact, ICT at this point is core to the industrial

infrastructure modernization agenda - transportation, retail and public safety are underpinned by IT technologies and networks. According to GE and the World Bank, the ICT innovation and embedding into our core industrial manufacturing will result in at least a thirty six trillion dollar opportunity or forty six percent share of the global economy over the course of the next ten years. While the G20 countries are looking at ICT embedding in infrastructures as the main lever of growth, the developing countries are also currently seeing 10 percent GDP growth and maybe more in the future.

That a global dialog on security is needed for ICT is not new. The worldwide recognition came about in the year 2000, with the year 2000 programming bug – when programmers hadn't thought about a four-digit year, but presumed two-digit years. The ICT industry did not know how to handle the zero zero and the turnover. There were incident response capabilities globally and as well as private-public partnerships merging to how to convert the entire computer infrastructure over to a four-digit computer code infrastructure so that the computers wouldn't shut down.

Then there was the recognition that key infrastructures, especially power, were more vulnerable due to the dependence of Internet and the infrastructure. There are control systems vulnerabilities that can turn on and off power grids. Cyber crime and cyber espionage or intellectual property theft are affecting the bottom line risk factors for many companies. It emerged right after the dot com domain came about in 85 and then, in mid 1990's cyber crime became more prolific. In the mid 2000's the Conficker worm of a general exploitation of the Microsoft operating system emerged. That necessitated international cooperation because core vulnerabilities of the main operating system, which got about eight percent deployment around the world, was leading to things like the Stuxnet or the Shamoon virus. Furthermore, cable cuts in the Mediterranean that caused Egypt to go dark have underlined the importance that the Internet is not just what's in the core infrastructure or geography or land, it's also under the sea.

Cyber activities generate impact. Their impact varies in more than a hundred countries that are cyber capable. Many of these countries as well as non-state actors are now starting to increase the role into domestic and international politics. And many countries are talking past each other. There are six ways to reason around this problem, which has gotten too complex and

needs to be broken down into smaller parts.

The first aspect is the amount of political activism on the Internet. The United States was very embarrassed by WikiLeaks and those trying to bring transparency to the US policies they didn't agree with. One could argue that Snowden's disclosure of data is also political activism, whereas in other parts of the world, there is political activism of using social media or the Internet in general to actually enable assembly to protest against the government and perhaps causing regime instability.

Political activism, though, is not the same as organized crime. Organized crime is prolific. Criminals are stealing personal credentials, credit cards, and real money out of banks. But that should not be confused with intellectual property theft. Intellectual property theft is the act of actually breaking in and illegally copying plans and intentions of your next generation technology. This is happening all around the world, against the actual trade practices that were agreed within the world trade organization and is economically damaging many countries.

In turn, intellectual property should not be confused with espionage. Espionage is action of state against state and is about stealing the plans and intentions of governments in regard to national and international aspects of policies for promotion of economic, political and military goals. Intellectual property theft and espionage are very different. In the United States the conversation, however, is bundled, which makes it very difficult to get to an international agreement - because many states, including the US, would not abandon espionage.

Disruption of services is yet another aspect - for example, distributed denial of service attacks on financial institutions. Such attacks are regularly conducted against US financial institutions, but also against banks in other countries, for example the South Korean Shinhan. The latest destruction of property, whether that is the Stuxnet virus or the weapon that was used against the Iranian nuclear power plant or the Shamoon virus that actually destroyed thirty thousand computers in Saudi Aramco - as a risk to a nation, or a corporation, have been taken seriously by the national and corporate leaders.

The tools that are being used for political activism or espionage or disruption are becoming more common. Such activity is reported on regular basis in many countries. Ensuring the resilience of companies and countries from these attacks, intrusions and activists is becoming more and more important. In fact it is on top of mind of many global leaders, the World

Economic Forum, commercial enterprises. Cyber crime was listed as the number one technological risk of 2012 and cyber attack is the number one problem in 2013, largely as a result of the Saudi Aramco event.

President Putin of Russia has also talked about the importance of bringing this dialog to a more inclusive body within the UN and the ITU and that this critical sphere of information exchange along cyber security is most important to be done in an area where all nations are represented. In India cyber security is discussed as an important part of overall government to citizen and business to business enterprises activity, and that it must be secured in order to enable the payments of employers and vendors, to enable the flow of goods and services.

President Obama talked about this as one of the most important economic and national security need the nation faces.

Accordingly, at least thirty countries have created cyber security strategies. Many of the European countries, as well as Israel, developed their strategies around the 2011 time frame. Japan published their strategy in June of 2013. It is not translated from Japanese yet and it's not available online. Japan's strategy was followed by India. One of the things missing out of everybody's strategy is the tie between economic productivity and prosperity and national security. Right now in these austere times countries are focused on the economic aspects, about embedding that ICT into every part of people's life because it promises productivity and efficiency. It is cored the modernization agenda and of course innovation is how countries are going to continue to prosper. But in the same breath and in those national security and cyber security strategies infrastructure protection is discussed, as well as intellectual property protection, defense of the homeland and in some countries even regime stability.

Countries are measured, and compared to one another, based on the implementation of ICT, by comparing broadband penetration, bandwidth, its price point and diversity, moving into the information society. Countries are therefore driven to migrate to e-banking, smart grids, employ new elaborate ICT systems – and are being measured by these efforts, which promise four to ten percent GDP growth. But are the liabilities being measured? From a business perspective the measuring is not based a digital balanced sheet. There is e-crime, IP theft, disruption of services, destruction of property and identity theft. The fragility in the less resilient of these critical services is causing this to be a national security conversation, but if the four percent minus

the negative is not measured then there will not actually be a national conversation.

The United Kingdom has published a report that said that, that they're seeing four percent GDP growth from ICT enabled services. They also have measured a minimum of three percent GDP loss to e-crime and e-fraud and potentially IP theft. Four percent minus three percent minus x percent is probably negative GDP growth, because the investments into security of ICT have not been assessed yet. The Netherlands republished a report by the knowledge organization for research and development TNO in early 2013, which assessed only two percent GDP growth in 2010, attributing a minimum of two percent GDP losses due to e-crime, e-fraud and intellectual property theft.

These examples lead to belief that the investments made over the last 30 years are not being realized, because the security agenda is not aligned with the economic agenda. In order to align them a strategy has to articulate the vision of combining and balancing both aspects, and it's not enough just to publish a strategy. If a strategy is not followed by an implementation plan, including specific attainable measurable with a result-based objective, then there is no vision to achieve. At that point, it has to be recognized that resources are scarce and that time is of the essence. The time battle is lost, execution and measuring performance are needed, as well as learning from own and other countries' mistakes. Out of the countries that have implemented cyber strategies, there are those with visions. Some of them have progressed and continue to implement their plans. Some are only starting with the execution but soon reverting because the strategy was not articulate enough.

As countries move forward with their strategies, they have to realize that the commitment and national resolve is not an election-based timeframe, nor an annual type of event, but is going to require a true investment over time and a commitment of resources in the competitive environment with extreme fiscal pressures. This commitment requires executive bandwidth, such as CEOs of major corporations and political leaders. It's also going to require real commitment of money from countries and companies, as well as political capital, because there will not be pleasant choices along the way. And of course time is of the essence. Instead of a "government knows best" regulation approach this is going to require true private-public partnership. Subsidization will be required, tax credits will be required and of course regulation will be required, but not at the expense of

other more incentive based market labors.

This is an international and global supply team and its global products and services are dependent upon each other. The next generation of innovation needs to be embraced, without creating unnecessary exposure to economy. Today e-government, e-banking, e-health, e-learning, next generation power grids, air traffic control, every essential service of all of our countries has been concentrated onto one infrastructure. There is no room for that one infrastructure to become fragile or become less resilient, making us vulnerable to simple attacks.

The recent decades, since 1969, have brought about great efficiency, forty percent productivity, and four to ten percent GDP growth. At this point we're seeing negative GDP growth, requiring measuring the declining gains in order to actually move the security agenda on the forefront of the economic agenda. And perhaps a readiness index of measuring that digital balance sheet is the way to move forward in order to be able to really realize the ICT dividend securely. And it has to be done together. "We really are intersecting highways," reads Sun Tsu and so we must join hands internationally and we must join hands corporately because we can only get and realize the GDP growth and the ICT dividend together.

Intelligence-Driven Security: A New Model using Big Data

Mr. Art Coviello | Executive Vice President, EMC, Executive Chairman, RSA

Einstein has been credited with the following expression: “The definition of insanity is doing the same thing over and over again expecting a different result”. In addition to the fact he never said it, the phrase has become a truism on its way to a cliché. But what if, what if you did the same thing over and over again wanting the same result and you stopped getting it?

Security practitioners have never been so anxious and frustrated as they are today, because the systems they’ve been using to great effect year after year are no longer delivering the same results. In fact, between 2005 and 2007, systems based on a reactive security model, focused on perimeter defenses, have grown increasingly ineffective. But although this issue has been discussed for years, it has not changed the behavior. For example, based on research commissioned by RSA, organizations are still spending 70 to 80 percent of their security budgets on preventing intrusions, largely around perimeter defenses, and only 15 percent to 20 percent to detect attacks in their environments, again weighted heavily towards the perimeter, and finally only 5 to 10 percent responding to attacks to prevent loss and disruption. This ongoing investment strategy is focused on a model that is clearly broken. The obvious question is: why does this persist? There are four reasons: budget - we’re used to spending that way, a technology gap - good alternatives for detection and response are only just coming to market, lack of information sharing at scale, and a critical skill shortage of cyber security personnel. As a result, those defending IT and critical infrastructure are confused, even fearful about what to do and

very angry. Angry at the situation itself, angry at governments for lack of coordinated action and angry at vendors for peddling an endless stream of faulty products.

To really understand the problem and what to do about it, three things need to be put in perspective: the attack surface, the threat environment, and how security models must evolve. Too often we focus solely on the evolution of the threat environment without considering the impact of technology adoption on the expansion of the attack surface.

It was only in 2007 that we really saw significant uptake in web front-ended apps. But today, in 2013, the common refrain is: there's an app for that, and by 2020 they'll be a deluge of big data applications, monitoring and checking and evaluating and analyzing everything about our personal lives and the world around us. And there'll be plenty of data to analyze, as we move from a quarter of a zeta byte to two zeta byte to as much as forty to sixty zeta bytes over that same time period – one zeta byte is the equivalent of 4.9 quadrillion books. We are gathering so much information day in and day out that it is literally being accumulated at an astonishing rate. And the reason we're going to have so much of this data is the number of people and things generating it.

The iPhone was launched in 2007 and today we have full mobile ubiquity. By 2020 we will have the Internet of things enabled by IPv6. Then, tens of billions, perhaps hundreds of billions of devices will be connected to the Internet. These trends have already taken away the primary element of our historical model for cyber security, the perimeter defense, that we're still investing in at a disproportionately high rate.

Already in 2013 we're in a hyper connected world that has facilitated excess and productivity for all of us but with the unintended consequence of doing the same for our adversaries. And if all that weren't enough, it's getting easier and easier with the advent of social media for our adversaries to trick, spoof, and assume our digital personas. Privacy advocates are worried about big businesses and big-brother governments infringing on their privacy, when criminals, rogue nation states, hacktivists, and anyone else who wants to, already is.

Given the reports in the US press recently, it is clear that we need to have a more constructive dialog about privacy. Governments have to explain why they need to do what they're doing to protect us, and how looking at vast streams of data to spot anomalies doesn't constitute eavesdropping on every single phone call or

email. And privacy advocates need to listen and understand this and then make their own arguments.

In the first two decades of the new millennium we will have gone from a cyber attack surface that has just a few points of ingress and egress through a controlled firewall perimeter to almost infinity, with regard to the impact of mobility, web apps, big data, social media and the internet of things. Our adversaries are going about their business over the same time horizon. Their targets and methodologies continue to expand, as their attacks get more complicated and coordinated.

Possibly more troubling is the evolution from traditional intrusive attacks to disruptive attacks, like we're seeing at the US banks with DDoS, as well as the Saudi Aramco attack in 2012. The evolution to these disruptive attacks is bad enough, but they also represent a serious escalation because they are the precursors to those long anticipated destructive ones. Despite the hype, destructive attacks are still next to impossible to carry out solely from the Internet without manual intervention. But as we transition to IPV version 6 and create the Internet of things, IP enabling more and more elements of our physical infrastructure, attacks of digital that result in physical destruction will become a reality - a chilling, sobering thought.

Taken together, the implication is that the ongoing expansion of the attack surface and the escalation in the threat environment require urgent action. There must be a sense of urgency to understand the security implications in everything we do, so that we develop and implant the right security model. The only way to reach and maintain the appropriate level of understanding is through knowledge. Knowledge from eco systems, from a much higher level of collaboration between public, private and vendor organizations, knowledge that will replace fear with confidence, knowledge that will guide our actions. Not surprisingly, the new model of security that we are advocating is intelligence driven to replace the ineffective, reactive and perimeter based model of the past.

Key requirements for such system are a thorough understanding of risk, the use of dynamic, agile controls to replace those outdated static perimeter ones, and a management system that has the ability to analyze fast streams of data from numerous sources to produce actionable information. To maximize effectiveness of those sources, we must get information both externally and internally. This means that we must become more adept at information sharing.

However, no matter how well we improve our understanding and management of risks, at best we'll be limited to understanding known threats and to a lesser degree known unknowns. An example of a known unknown is being aware that vulnerabilities will increase as we increase the level of excess and amount of data being exposed through mobile devices and BYOD. But an unknown unknown is something we couldn't have had, because knowledge of that could create an adverse condition. And we'd be wise to understand that this is going to be an inevitable consequence of change and of the dynamism from the ongoing acceleration of technology adoption.

So how does one build an underlined system that can anticipate and spot an unknown unknown threat? Can we even architect an intelligence driven model that is future proof? It's not a matter of perfect security, but a model that allows us to detect attacks and respond quickly. Big data makes such an intelligence driven model viable. Big data is the recent years buzz word, therefore it is important that we define it: fundamentally, it implies the ability to extract meaning, to sort through the masses of data elements and find the hidden patterns, the unexpected correlation, the surprising connection. It is about analyzed fast and complex data sets at high speed that in our case will allow us to spot the faint signal of an attack, because at some point, no matter how clever the attacker, they must do something abnormal.

In an intelligence driven model big data will be applied in two ways: in security management and in the development and application of individual controls. Security management systems must be able to gain full visibility into all data, unstructured and structured, internal and external. Underlined big data architectures will be scalable enough so that all data can be analyzed, no matter how extensive or fast changing. As a result, organizations will be able to build a mosaic of specific information about digital assets, users and infrastructure, allowing the system to spot and correlate abnormal behavior in people and in the flow and use of data. The management system must be well integrated with the GRC system and tasks specific tools so that we can detect those attacks early or even in advance and then trigger automated defenses such as blocking network traffic, quarantining systems or requiring additional identity verifications.

As to the controls themselves, because they have so much information, big data controls will be smart to begin with. They will also have the capacity to be self-learning and be able to inform or be informed by other controls. They will also be able to

feed or receive intelligence from security management systems and report to and receive instructions from GRC systems. Armed with a thorough understanding of risk at the outset, this big data oriented management and controlled environment completes a vision of intelligence driven security.

Aside from technology, action on the part of boards of directors and C-level executives, practitioners, governments and vendors is needed to make this model viable. Boards of directors and the C-level suite need to recognize the responsibility to be educated so that they will have a clear level of understanding. They should set the tone for evaluation and management of risk and they should ensure that risk is managed on a more granular basis throughout the organization, not just in the IT and security groups. And last, they need to be in a position to make intelligent decisions so that appropriate resources are available to the security organization. For security practitioners, there are three recommendations: first, to look critically at those budgets, design a plan that transitions the existing infrastructure to an intelligence driven one, migrate for point products to a unified security infrastructure using big data controls. Implanting these tools will give a true defense in depth. Next, to strengthen operations data science skills by adding data science, scientists or outside partners to manage the organization's big data capabilities and to overcome the skills shortage. And last, to leverage external threat intelligence augmenting internal analytics programs with external threat feeds from as many sources as possible.

Furthermore, governments need to unite security professionals, domestically and internationally. They also need to implement national strategies based on lead by example, on solutions for own problems, because there is so much at stake for the protection of critical assets and infrastructure. Governments also need to facilitate information sharing by acting as a central clearing house to exchange information about current threats and attacks. Big data applications will only be as good as the data itself, and sharing of external threat feeds will have a force multiplier effect in our environments.

Regulation should also be an important element of the strategy, but governments will never keep up with the pace of change of technology in the threat environment. Regulation therefore should focus on outcomes and not proscriptive measures. If they must prescribe, they ought to do so around best practices that can be applied to fit multiple cases, using a variety of technologies. Also, they need to help with the serious skills shortage of cyber

personal by fostering and funding security education programs to produce the human resources that are needed.

Governments also need to cooperate internationally and extend information sharing among networks of countries. This will facilitate the tracking and capturing of adversaries. Further, they need to jointly develop rules of conduct around intellectual property, which is fundamental to globalization in e-commerce.

Finally and most important, we need to eliminate the prospect of destructive attacks and cyber warfare. Vendors must work to close the technology gap for defending what the expanding attacks surface and escalating threat environment has created. They must stop enable customers to migrate to an intelligence driven model as quickly as possible by stopping the steady drip of point products and ensuring that they take a big data approach to the controls. They too must cooperate so their technologies work seamlessly in their customers' environments. Historically, the benefits of security infrastructures have been in the ability to react and act against known threats – an approach that no longer suffices. Only enabled by big data intelligence driven security will also have the ability to act against both the known unknowns and the unknown unknowns. As President Peres said, "We must never be satisfied", but we should at least be able to keep pace with our adversaries and in many instances get ahead of them. But this will only be possible if all constituencies work together in a collaborative eco system for a common purpose – to make sure that technology is used for the benefit of all of us.

Building Cyber Warriors

Mr. Paul de Souza | Founder & President, Cyber Security Forum Initiative (CSFI)

In the US there are around 3 million IT professionals, and sixty one percent of those fear Anonymous because of their lack of knowledge and preparedness. Cyber space is a warfare domain. It can be used as a weapon and in military operations. If we don't understand our capabilities and don't know how to operate in cyber space then we do have a problem, lack knowledge and understanding of how to fight in cyber space.

Several resources are needed to create fearless cyber warriors. First of all money is needed. We have to have enough money to train our cyber warriors, and since the situation changes every day, they have to be trained constantly. Second – time is needed. Unfortunately, there is not much time.

The US requested and got approved a budget of 4.7 billion dollars for cyber operation in 2014. It is unclear whether this amount is sufficient, but if used wisely it can contribute to training lot of cyber warriors with a solid experience in building networks, defending networks and operating in cyber space with full spectrum capabilities. This implies the full spectrum from computer network attacks, computer network defense to computer network exploitations.

There needs to be solid expertise. To start with, in building a network from the ground up, running the fiber, setting up the servers, IDFs, IPS, firewalls, proxy servers. It is a lot of work, but it is a good start because it is not hard to find network administrators with these kinds of skills and expertise. Then, these cyber warriors need to be able to defend those networks, to create security controls, rules for firewalls. They need to

be able to monitor those networks in real time, to understand what's going on and to have the situation under control. These tasks take a lot of skills, on top of building the networks – and there are significantly fewer personnel who possess these skills and capabilities. Crucially, it is not only the military that needs this kind of expertise. The concept applies across the broad spectrum. In the private sector, the industry, there is a need for cyber warriors. General Alexander says that cyber warriors are skilled for and capable of, again, full spectrum cyber operations. We do not have the choice to unplug the networks but have to be able to fight through an attack. We have to be able to keep the network running, because employing a kill switch to go offline when attacked is not an option anymore. The current Joint Publication 3-13, the doctrine for cyber operation, gives an insight into how the US goes about cyber operations. This doctrine was publicly released and can be downloaded from the Internet. However, the details of offensive operations are included in a classified, new doctrine. On the matter of what a cyber warrior is David Dittrich says “well you know you have to have more than ten years of experience at the highest levels of computer network operations in order to have cyber defense and offensive capabilities.” But there are not many personnel who actually have ten or more years of experience in computer network operations.

The following are some of the new unclassified terminologies from the new doctrine for cyber space operations.

They show that things are changing from just a defensive position to active defense and offensive operations.

It takes a lot of skills to become a cyber warrior. It is about dedicating a life to the matter, understanding the full spectrum of cyber operations, the law and policy of armed conflict in cyber space, doctrine. It is more than just cyber security, which is just a small fraction of cyber operations. It seems like Israel is taking the right steps in creating cyber warfare units, but it has to be kept in mind that it is constant work. It takes time, skills and it takes a lot of money but it can be done.

Leveraging SDN for Network Visibility, Security and Threat Response

Mr. Robert Shaw | CEO and President, Net Optics, Inc.

There is the potential to make a dramatic change in the cyber industry. However, there are some big challenges. The first challenge is that the approach used today for network security is not working. The second challenge is that vendors and suppliers need to change the way they are thinking about the world, because in many cases incremental change and point solutions dominate instead of revolutionary change and great breakthrough. On the following pages I will introduce an approach that presents a new way of looking at the world, which evidently leads to better results, because in order to win in the war on cyber attacks we have to take a completely new approach.

Net Optics opened an R&D center in Israel in order to be able to leverage from the best and the brightest talent in the country, to be used as a springboard not only to Israel but also to Europe. The R&D center became a huge success: starting out with 20 talented skillful individuals, the center grew, and continues to grow with doubling sales. The VP of technology, Sharon Besser, and the VP of engineering, Shlomo Gurfinkel, have built a team that has focused on how to win in the cyber space. In order to win, some change is needed.

First of all, the logos that are flashing across the top are household brand names and they have suffered breaches in security. A hundred and thirty major incidents have been reported to date. In the first half of 2013, seventy percent of these were discovered – by individuals other than the organizations themselves, and in most cases it was by one of the consumers. That does not present promising statistics, and forty four million users were

compromised.

Net Optics has a different prospective to look at the world. Those familiar with Net Optics, know that the company forms the backbone in some of the largest organizations around the world, providing products and services that are sitting both in the largest government agencies and the largest enterprises. The company has seven thousand customers and all of the data from the networks runs through Net Optics' products in order to feed the security tools. Therefore Net Optics is able to assess how current and future networks look like typically better than anyone else in the world. Based on these assessments, and conversations with customers, whether it is a CIO, CTO, CEO or the head of a large military establishment show worries of whether the way organizations are thinking about and deploying their security solutions is not right. These organizations are facing their tools becoming overwhelmed with the result they cannot keep up. The reason for this is that they do not think about an architecture that is completely different, a security-centric network. A network that is designed based on security from the very beginning so that the DNA of the network is constantly thinking in a different way, not dependent upon one particular tool in order to handle it.

Total visibility across the network is key and one of the challenges that most organizations face today is having a data center as well as a cloud and virtualization environment - organizations are trying to build a security centric network and establish visibility across both of those important infrastructures at the exact same time. There needs to be total visibility into all of them, ensuring that the industry standards are utilized. Additionally, there is a need to be very clear managing both of these very important infrastructures providing simple, centralized management. If these requirements are not implemented, the tools will continue to become overwhelmed.

Typical security deployments today follow a general routine: one – customers have deployed security solutions, the best of the class and they've said "you know what, what I'm putting in the network today actually took two years to engineer, design and release so from the time I have it, it's actually outdated". This means that outdated innovations, point solutions are being deployed, while facing advanced threats on many vectors making it impossible to handle zero day exploits, which results in a security tool that instead of solving the problem now becomes the risk and, as agreed earlier, time and resources are limited.

Net Optics approaches the problems in the following way. One – high availability, knowing that there are critical spots of the network, what's typically happening is costumers are actually deploying two or three security devices in certain areas to make sure they're covering it. This results in complex deployments, mesh type of networks for the sake of the ability to handle any type of threat and being very responsive or constantly innovative, employing the latest and greatest technology to try to anticipate anything what happens, not necessarily knowing what it is. The alternative is to continue to invest and spend. This results in the recommendations and deployments being a concept where the actual network becomes part of the solution.

Imagine for a second if the network could make decisions on its own. When it saw that in a particular area the amount of traffic or the patterns started to become unusual and as a result could redeploy tools itself, without human intervention. It could take what is typically one or two security tools that are targeted to that particular part of the network and repurpose and redeploy four or five others. That would be possible because it would know that the attack coming in the next minute was something that it hadn't prepared for and the current tools that were targeted to it would not be enough.

This is currently being done today and it is a completely different way of architecting visibility and security into the network. The other aspect is how to cover all the various corners of a network, providing not only visibility into what is happening but also to be able to take action on whatever transpires. One of the key pieces of this is that as the network is designed both from a cloud and virtualization as well as from a physical standpoint, there is no clarity of where the breach in security is going to come from. Instead, tools are needed that are able to repurpose themselves in real time so that they can handle the unforeseen attacks.

Such networks are being designed, with three or four security suppliers sitting in a conference room together with the costumer, architecting the network. There are APIs that are starting to be shared so the infrastructure becomes a living, breathing, operational, security structure, so that they can be responsive, proactive, and take action in a very quick manner.

It can move quickly, it can anticipate what's going to happen and it can take tools that were originally targeted for certain part of the network and redeploy them wherever needed without human intervention in a very quick, timely manner. For example, there is threat entering into the network, the centralized controller

identifies that something unusual is going on and promptly makes sure that the current tools are being deployed correctly. This strategy goes down to the network packet broker and actually reconfigures the network, reconfigures the tools and allows the tools come into play to take action on what it is needs to happen.

In the past, without configuring the network as security-centric, whenever an attack became too big for the existing tools, customers needed to call in help, take down parts of the network, shut things down, take some actions. It's impossible when dealing with the scale and scope that persists today to be able to do that. Instead, out-of-the-box thinking and designing in a completely different way is required.

The key attributes are focused, they're really important:

How to approach total visibility across the entire network in order to be able to respond quickly?

How to easily prevision the information that is needed in order to respond?

How to develop standards across what everybody is doing so that in fact energy, ideas and insight is combined?

Making sure that it is simple and centralized before providing the solutions, and in fact we are clear in separating what is done from a monitoring standpoint and what is done for a security enforcement standpoint.

Net Optics has a number of the products that are being used, not only in Israel but around the globe, that are making a huge difference about the security centric network that can be vetted and used as an example.

If we band together, we can change the world.

Wifigate - How Carriers Expose Us to Wifi Attacks

Mr. Adi Sharabani | CEO, Skycure Security

Okay, so what I want to talk to you about today is these devices. How many of you are currently holding a mobile device in their hand? A lot of people, right? So it's not just holding them, obviously a lot of us have them in our back pockets and in the bag. Specifically, in Israel we are commonly a bit ruder, so we can hold them and use them during presentations. Please don't do it now because there was a kind of attack that happened here which I will illustrate later.

In Skycure we focus on the problems of mobile devices security, specifically for organizations. Looking at the actual current threats shows that the available solutions are inadequate in addressing those threats and that there is a huge technology barrier. At the end of the day what we see is that mobile is actually the best entry to hack into the organizations, to hack into the employees of the organizations and leverage their devices to perform other more malicious activities.

Skycure has discovered a new type of vulnerability: The problem is a known problem called Wi-Fi attacks. Generally speaking it is known that connecting to Wi-Fi networks might put the user at risk for many different types of attacks, for example a man-in-the-middle attack, which is a well-known concept. However, there are two main challenges to perform a successful man-in-the-middle attack. In most cases, the attacker needs to be close by. This means that a person in China cannot perform this specific attack on someone located in Israel. The second element is that the user needs to do something – connect to a Wi-Fi network in order for an attack to be performed on the

device. However, Skycure earlier disclosed the first persistent IOS malware that allows performing the attack remotely – the attacks are not necessarily local anymore.

The second element is the action on the part of the user. The challenge is to think from the hacker's prospective. Try to hack into someone that hardly ever connects to Wi-Fi networks, but it is actually very simple. There is a great feature in mobile devices called auto connect. At home or at the office, the device automatically connects to the networks that exist there. That means that if an attacker can just anticipate or guess, which networks the device ever connected to, and create such networks anywhere, then the device will automatically connect to the attackers' system and she will be able to perform all the known attacks on the device.

The third element is an even a more challenging problem. An executive of a large organization said that he specifically hardly ever connected to Wi-Fi network, and by hardly ever he means he only connected to the Wi-Fi networks of his office. This means that if not a directed attack on his specific organization is performed, attackers would not be able to guess the Wi-Fi network that specific single Wi-Fi network on his device. However, what Skycure came to learn is that his device actually has more Wi-Fi networks configured on: In practice the mobile carriers themselves are capable of setting configuration on devices, those configurations were created mainly to allow phone calls and data connection over the 3G or 4G network.

However this technology could allow them, and in practice they use this technology, to specify Wi-Fi networks on the devices. There are different bundles and carrier settings, including Wi-Fi network that are automatically configured. In the carriers sometimes also provide Wi-Fi networking. This allows them to do offload of the 3G or the 4G expansive data plans to Wi-Fi. For example AT&T has a lot of hotspots around the world and many other vendors do as well.

The issue is clear: if such a Wi-Fi is maliciously created any user of that carrier will automatically be connected to this Wi-Fi, allowing the hacker to perform attacks on their devices. This means seeing sensitive information, stealing credentials, in many cases viewing email credentials. As it is widely known, hacking into an email account is actually giving the attacker the secret key to the entire digital life, because there is always the option of "I forgot my password, please send an email to my email account to recover that password or to create a new one".

One of Skycure's customers' IOS devices connecting to a network in Brooklyn, resulting in alerted malicious activity within that particular network. Indeed the Wi-Fi network associated with one of the bigger carriers in the US and Skycure was provided with a location. At first, it seemed that that someone also connected to that legitimate Wi-Fi network, and performed attacks on that network. However, a closer look revealed that this was not the case. The carrier has a Wi-Fi service locator, listing the hotspots around the world for that specific Wi-Fi name. The closest Wi-Fi that exists under that name was seven blocks away and out of the reach of the Wi-Fi of the IOS device of that customer. This means that someone created a Wi-Fi code under that name and performed that activity on it.

It is unclear whether the attacker fully understood the ramification of this attack. They might have guessed that if they will create a Wi-Fi under that name, many people will connect. However, in practice, any passer standing in that area that is a user of that carrier, was automatically attacked.

After this event, Skycure decided to put the system to the test. Equipment which costs about 30 USD, was configured to create several Wi-Fi's that otherwise are used by various carriers. Thereafter the device was placed in a conference room, aiming to monitor, how many devices will automatically connect. In the matter of 2,5 hours four hundred and fifty devices connected to this Wi-Fi. In this case, Skycure did not aim to, or performed any attack. However, an attacker would be able to do it seamlessly without the knowledge of the user.

This is a tough problem because this problem results from the design of the Internet. Problems rooted in the design of the Internet are much harder to solve. In practice, there is currently no best solution for the consumers. Companies like Skycure are trying to solve these problems for organizations, but not for regular people. One small action users can do is if they are using an IOS device, is to simply turn off the WiFi on the device when not in use. However, that is a somewhat problematic and maybe counterproductive solution. Another option is to use a mobile firewall. There are some companies that are focused on consumers provide some protection against some of the threats listed here.

Carriers or a Wi-Fi network providers need to make sure that when they provide a Wi-Fi to supply it with a firewall in place, so that all the clients that will connect to it, whether they are mobile or not, will automatically enjoy a seamless security model that

will protect against the current threats that we see out there in the world.

02

Second Session: Cyber War & Peace

Cyber War, Cyber Peace

Mr. Richard A. Clarke | President, Good Harbor Security Risk Management, Former Special Advisor for Cyber Security to the President of the USA

In the 1990's, the US State Department worked hard to convince Israel that there was a role in Israel's security for arms control. It was not an uphill fight, but over time Israel recognized that there was some value in arms control. Arms control is seldom mentioned these days in the same breath as the word "cyber", but there is room to propose to start thinking about it a lot more, thinking about cyber peace through the concept of cyber arms control. With experience from both cyber policy and arms control, it can be argued that a connection between arms control and cyber security is possible and should be built. This article describes why and how it should be built, as well as where to start.

Sometimes it is difficult to fully appreciate or remark upon significant events, or to put the news flow into perspective. In June of 2013 something momentous happened in the issue of cyber security in little place called Rancho Mirage in California. Arguably the two most powerful men in the world, the president of the United States and the President of China, sat down together for one-on-one talks about their major bilateral issues. One-on-one talks between the US and China have happened before over the course of the last thirty years, but this meeting was the first time that the number one issue on the agenda was cyber security.

Two to three years ago, when some advocated getting that issue on the agenda it was difficult. But in the wake of the cyber attacks that have occurred in the United States and throughout the world in the course of the last couple of years, now the agenda item of cyber security is number one in US-Chinese discussions.

Naturally, during the first meeting of these two men to talk about cyber security there was no agreement. The United States accused China of industrial espionage attacks, launched by the People's Liberation Army, the army of China, against American and European companies as well as companies throughout the world. The Chinese president responded that China too was the victim of many cyber attacks. He also denied a lot of what the United States alleged was coming from the Chinese government. Thus progress was not made, but the two men agreed to put the question on the agenda again, to have working group discussions in the meantime and to try to develop rules of the road for both nations' activities in cyber space.

Rules of the road are another way of describing arms control and therefore it is helpful to step back for a moment and think about arms control, what it accomplished and where it began. When arms control began in the 1980's and the 1990's it was universally greeted by the media, by academics, by commentators with skepticism. They said arms control between the United States and the Soviet Union, on the multi-lateral global or regional basis such as in Europe was just going to be hard. There were technical issues involved which diplomats could not understand – technical issues about engineering, about missiles, about satellites, about telemetry, about nuclear physics, biological sciences. This was going to be too hard to get into a diplomatic agreement and moreover, people said, the other side will cheat. You cannot get verification of anything that is significant and, they said, no one would agree to limit anything of significance. The United States and the Soviet Union proceeded over the course of twenty years to negotiate very difficult, very technical agreements, with very intrusive verification measures, including “anytime- anywhere” inspections in each other's countries, lots of advance notification, lots of exchange of information, lots of confidence building measures. And they agreed to treaties to limit nuclear weapons, to destroy nuclear weapons, to limit delivery of defense material and to limit nuclear tests – all on the bilateral basis.

On the multilateral basis, the United States, the Soviet Union, Europeans and others agreed on treaties to abolish biological and chemical weapons, to engage in confidence building measures

regarding the conduct and the activity of military forces. Also, vast withdrawals of forces from central Europe were agreed upon. All of that made a lot of people safer. It is worth remembering what was accomplished, and it's worth remembering that when the nations started out on the process they were told that it could not be done, just as we are told today that cyber security does not lend itself to arms control. People say that cyber arms control is too technical, that diplomats do not understand it – and that is largely true. They also say that such control cannot be verified, that there is an attribution problem. But the attribution problem is overblown, in point of fact governments, intelligence agencies can most of the time figure out who is engaged in cyber attacks. Despite spoofed identities and difficulties to exactly identify every instance, most of the time cyber intelligence agencies can figure out who is behind the attack, making verification is possible. There is no 100 percent requirement; it just has to be adequate.

What could cyber arms control look like? What is a possible starting point? One of such starting points would be a mutual international agreement not to attack the financial services sector – banks, stock markets, and alter financial records or alter bank accounts. No government in the world today seems to be doing that. Cyber criminals may have interest in such activity, but not governments. In fact, in 2003 as the United States was getting ready to attack Iraq, a group of advisors went to President Bush and said to him “before you attack Iraq in physical space, you can attack it in cyber space”. “We have the capabilities”, they said “to hack into the Iraqi banks and to transfer funds from the Iraqi banks to our own, ensured by hacking we can make Saddam Hussein pay for the American invasion.” It sounded like a good idea, until the involved realized that the international finance and banking center depends on trust, confidence, on believing those numbers. And numbers in the banking center cannot be trusted, the bank cannot be trusted, if those who own that stock cannot be trusted, if the price when that stock was traded cannot be trusted, then the whole system begins to unravel. And so President Bush, who very seldom made wise decisions, made that wise decision to let Saddam Hussein keep his money for a while.

Because no one is engages in such activity, this is a possible point to start creating cyber arms control. In the history of arms control, it begins by having countries agree not to do things that they are already not doing, things that they do not want to do. This makes an international pledge not to attack the financial services sector and change the numbers a feasible starting point.

From there it is possible to going back over a hundred years of arms controls treaties to not using cyber weapons to specifically to target medical facilities. Attacking a medical facility, altering, scrambling medical records to change the patients' blood type could result in many deaths and could result in destabilizing the entire medical system in a city. These are the little first steps that can be taken.

In the larger picture, an international system is needed, that allows a nation that is under attack, a DDoS or an advanced persistent threat attack, to report that attack. For example, if Israel determines that a DDoS attack against an Israeli bank is emanating from a server in Cairo, Israel should be able, through an international system, to say that an attack is ongoing. It should be able to tell the government of Egypt, which should have an international obligation to respond, to assist in finding that server and shutting it down. There should also be some sort of international secretariat that will record the action, the date and time of Israel reporting the attack, as well as how well the government of Egypt did in responding to the resulting request. In this way, over time there will be a record of what nations are cooperating, what nations are honoring their international obligation to assist and what nations are not. There is also room for sanctions, some response to nations that are not cooperative. That international secretariat that recorded these requests for assistance could do other things. It could have, like the IAEA, the International Atomic Energy Agency, international inspections teams that would be available to provide technical assistance to countries under attack – Estonia needed such assistance in 2007, Georgia needed it in 2008. That international team could also include a group of international forensic experts that could go into a country like Estonia in 2007 or Georgia in 2008 and try on an international basis to prove where the attack came from, providing proof for what nation was violating international agreements and international understandings.

There are parallels like the IAEA and there are parallels in other organizations that aren't specifically tied to arms control. For example, money laundering was a problem for narcotics and terrorism. A group of like-minded nations got together and created something called the Financial Action Task Force, a very light, thin, international body, not a big UN bureaucracy. And the financial action task force began by agreeing among themselves, based on the standards for anti-money laundering laws. They came up with an international standard that all nations in the

group then implemented as domestic laws, saying what they would do to combat international money laundering. Then they audited each other to make sure that each nation was honoring those commitments. As the next step in the process this group of states required the outlaw states to implement and enforce similar laws under threat of no longer clearing these money laundry havens' currencies. This way it was not only one country, such as the United States, engaging in a diplomatic protest. Instead it was a group of the fifteen largest economies in the world at the time going to these money laundering recalcitrant states and saying either you live up to these standards that we have created, or we as a group will impose sanctions upon you. There is a lesson in financial action task force for how arms control could be dealt with in cyber space.

To date the discussions of arms control and cyber space have been in a UN forum. A forum, which nations like Russia and China have largely used for propaganda purposes and to make political points. Therefore, the UN is not the place to start cyber arms control. Instead cyber arms control could begin similarly to the strategy for money laundering, with a group of like-minded nations who could set up standards for behavior, agree to mutual obligations of assistance. These nations would have to pass new domestic to enforce those standards. For example, if Israel finds that there is server in Houston Texas that is the source of malware attacking here in Israel, the United States will have to have a law in place, which it does not today, to take that international request for assistance and to be able to quickly, within hours, go before a judge, get a warrant and go and seize the server. That cannot happen today, but if there was an international agreement, even an informal one, than domestic legislation like that could be passed. If these understandings about rules of the road were in place among a group of like-minded nations, than it would be possible to act similarly as was done with states who did not want to follow anti-money laundering standards. The like-minded group of nations could say, "stop this kind of activity or else", and then develop sanctions just as it was done in various other arms control and other international agreements.

For example, if there was a nation that consistently engaged in cyber espionage or had become a haven for cyber criminals, a nation that was a scoff-law, not living up to the international standards that were agreed upon, then the like-minded nations could do several things. They could deny visas to people from that country as a first step, the low end of the spectrum. At the

high end of the spectrum, if there was a nation that consistently engaged in cyber espionage and in breaking international norms, the like-minded nations could limit the bandwidth going in and out of that country. Of course that would be difficult to do, expensive and difficult to agree upon, but the price the world is paying today for cyber crime and cyber espionage is a very high one and therefore it is not inconceivable at all that a group of like-minded nations would refuse to connect to that country anymore at a high bandwidth. In fact, every packet going to and from that country is going to be inspected, scanned, slowed down and quarantined. It is technically difficult, but not impossible.

The threat of that kind of international action by like-minded nations may actually result in progress on agreement to international norms and obedience to those international norms. The meeting between the United States and China in June of 2013 was momentous, even though the media didn't cover it quite that way. It was a momentous step in the history of international diplomacy with regards to cyber security. Still, there are many more steps to take and the history of arms control in the 80's and 90's tells that these journeys can sometimes take ten or fifteen or even twenty years to negotiate and implement. But these journeys are worth it because if history is a lesson, international agreements - while they are not a panacea or a substitute for national security programs - they can minimize and mitigate problems and contribute to national security as well as international stability. They are not an overall solution, but something worth doing.

Nations need pause and go back and study the bi- and multi lateral arms control processes of the 1980's and 1990's, learn the lessons from that recent past and then think together about how international arms control agreements in cyber space can be crafted. There are skeptics, but twenty years from now we will see what great progress has been made. People will make it. And as for the United States, my message is "fine, have talks with the Chinese, have talks with the Russians, have talks with the UN, but really if you're going to start and make progress, first have talk with like-minded nations, have talk with your friends, start with your friends. And the United States has no greater friend than Israel."

The Attribution Problem - A Fresh View

Dr. Thomas Rid | Reader in War Studies,
King's College London

A cyber attack has never resulted in a single physical injury, let alone fatality. Usually it is something else. The only cyber attack that has resulted in significant physical damage was Stuxnet, and therefore the argument is that focusing on Stuxnet makes it more difficult to talk about the proper solutions. Therefore, the notion of war in cyber is counterproductive because the terminology is not used as a metaphor, as in the war on cancer, and the war on drugs, but to signify violent or at least potentially violent acts. But indeed, if it can't kill it is not really an act of war, but an act that is instrumental. It is done to change the adversaries' behavior in a certain way; it is also political in a sense that an actor takes credit for the event, saying "I did this to you because I want you to change your behavior". In few cases of cyber attacks meet even one of these three criteria, and arguably none meets them all. So if it's not war, what is it then?

If there is a focus on war and weapons in this context, there is also a focus on two things: one, the military should be in charge, or at least a military organization or an organization related to the military, and second, violence. This results in all these science fiction scenarios of very bad things happening, planes falling from the sky etc. While these scenarios are not entirely impossible they are unlikely to happen any time soon. Instead, what persists is sabotage. Sabotage means that a computer attack is conducted in order to make a machine stop or damage the machine, as Stuxnet did, or, more abstractly, damage a process, withdraw efficiency from a process. Sabotage can relate to a bureaucratic process as well, but it has to be immediate, not over a decade.

Second is, sabotage attacks, and again, these are the exceptions. It depends on what is regarded as such, but focusing on industrial control systems, given the data and case studies that are available, there have been only three to five attacks that were actually successful and made a difference, Stuxnet being the most important one. It is a tiny number and in the context of sabotage it makes sense, to speak about cyber weapons or cyber arms that could be controlled, again like Stuxnet. Common devices or code can turn into weapons only if they have the potential to actually create a sabotage impact.

The next activity that needs to be mentioned, if very briefly, is espionage or intelligence operations. Intelligence agencies do not like to use the term 'espionage' if they are talking about themselves, only when they talk about others. Espionage is a major problem, of course that is not controversial to say – economic espionage, commercial espionage, intellectual property theft, but of course also political espionage. And in the cold war nobody tried to ban espionage. Indeed, even today it would be rather unrealistic to assume that western nations would limit their espionage intelligence operations in this arena significantly. Therefore, in that context, it doesn't make too much sense to speak about arms control, because, again, information that is used to extract information only is probably not a weapon, only once it is used to start influencing a process.

Hacktivism and subversion need to be mentioned as further types of activities. These however go beyond the scope of this paper. There is also the aspect of crime, but talking politics in this paper, crime is only mentioned for the sake of completeness. Instead, the key argument is that in none of the three areas there is more violence, weapons, cyber war or acts of war. On the contrary, there is less violence. Today it is possible to sabotage or blind the air defense system, as Israel allegedly did in 2007 in Syria through computer attack. There is no need to kill or injure the operators of that air defense system; it can be done by code, a by a computer attack only. It is rather difficult to do, that is why it is so rare, but in theory it is possible, resulting in no violence in some acts of sabotage at all. This is a new distinction today, which is cleaner than in the past.

Similarly, in espionage, it is possible to obtain information without engaging trading operatives first, from a distance, therefore the personal risk involved in computer espionage is arguably is much lower than the personal risk that people took to dig the Berlin tunnel, or to bug an embassy in the cold war. This means

that even in espionage there is a new physical less of violence dynamic at place.

Thirdly the same applies to subversion and crime. Crime statistics show what the world is in the middle of an economic slump. In the UK crimes statics were released in the first half of 2013 and it happens to be that, quite surprisingly in this economic climate, almost all forms of street crimes, are down, while, of course, computer crime is up. This leads to believe that the dynamic of “more cyber, less violence” may apply even in that field.

Weaponised code, or cyber weapons, could be possibly limited, and the only example that there is so far is Stuxnet. There is nothing like Stuxnet, so whoever mentions “attacks like Stuxnet” should be met with skepticism. Not even Flame or Qatari RasGas attack or some espionage operations that may have used code that was used in Stuxnet come even close because they don’t have a highly specified payload that was developed for an ICS system. Still, even Stuxnet failed. It was a good idea, but unfortunately it failed and there are five reasons for this failure.

First, it failed because it was a psychological operation primarily. The idea was to mess with not just the equipment of Iranian engineers but with their minds. If one thinks that they cannot complete their work, than it is very hard to find a solution, because the person who is supposed to solve the problem is the problem. On the other hand, if it is known that somebody else is causing the, then it can be isolated and finally solved. By the time Stuxnet was found as software, or as attack code, that had happened. Lack of attribution did not matter; they only needed to know that somebody else caused the problem.

Secondly, the physical or kinetic element also arguably failed. The sabotage dimension also failed because an analysis of data publicly available from the IAEA shows that only the first wave of attacks that started in June 2009 had an impact on the number of centrifuges that were online at the time. There were four thousand nine hundred and twenty centrifuges online, if those data are credible. And they dropped significantly by approximately a thousand. The problem is that these numbers have to be put into context and the drop cannot be fully attributed to Stuxnet. Bottom line is that overall the Iranian enrichment capability did not significantly dip and the ability of the Iranians to install and run new centrifuges did also not dip but is continuing to climb. Therefore Stuxnet may have been counterproductive because it, thirdly, improved Iran’s defenses, because Iran is now better prepared to deal with similar attacks, should they come again.

Iran also certainly hardened its system and also it made it more difficult to gather intelligence on their operation.

The fourth reason, and it is connected to the third, Stuxnet improved not just Iran's defensive capability when it comes to its nuclear enrichment program but also Iran's offensive capability. The intelligence communities in different countries assume that Shamoon, the attack against Saudi Aramco, that the attacks against American banks, DDOS attacks are Iranian operations. There is no proof of that, at least on the public domain information is not available, but well-informed people make that assumption. If a country finds itself at the receiving end of the most sophisticated computer attack ever, it is to be expected that the country will be doing something about defensive and offensive capabilities.

Finally, the fifth reason is that Stuxnet redefined the rules of the games. It is now okay to do offensive operations on a major scale. And that is rather ironic that the United States and Israel together, as publicly credited for the operation, achieved this affect. In a secret presidential directive, that was leaked to the press, the White House states very clear that, that Stuxnet created a number of counterproductive side effects – although the document does not talk about Stuxnet explicitly. From an Israeli point of view one of the most unpleasant side effect is that many people outside Israel think that something was done about the Iranian nuclear program, but in contrast to concern about this program Stuxnet did not really do that much. It was a feel good operation, a good try, but a kinetic operation may have only been slightly delayed by it and may still be necessary at some point.

The point here is that focusing on the offense, on cyber weapons and on cyber war is weakening the defense. As well as hyping the offense is weakening the defense. For example, most of investments at cyber command in Fort Meade that were announced in 2013 are on the offensive side. Yet, investing personnel and skill on the offensive side does not make own networks any safer. As a result of the hype on the offense it is more difficult for the defense, for the Department of Homeland Security, for ICS to recruit the skilled people that these intrusions would need. The offense is just sexier than the defense. If the professionals are not working for Google, they would rather work for the NSA, not the DHS, which constitutes a significant problem. Given the overall amount of control system devices, critical or not, that need to be defended, focusing on the offensive, or even on active defense, as currently is the discussion does not do anything to provide safety. Should something serious happen, a serious

cyber attack, where actually people get injured or killed, a few people would ask: “well, did it actually make us any safer to focus on the offense and leave all these systems so badly secured at home?” The answer is clear – it did not.

Building an Effective National Cyber Defense – Capabilities, Strategies, Policies

Mr. Ilias Chantzos | Senior Director, Symantec Government Affairs–EMEA and APJ

It might be a better way to spend our time on what do we actually need to do about defending ourselves, rather than focusing a discussion on arms control or offensive or warfare. How is deterrence possible by denial? How will it actually be possible to stop the cyber attack?

Recently cyber security has been catapulted to the political significance level, people now argue that cyber is a number one threat. The situation changed this way after a number of major security incidents that have affected countries and infrastructures. These incidents made people understand that the threat is very real. Estonia back in 2007 was a wake-up call.

What is cyber being used for? What do people do when they are launching their cyber attacks? How are these affecting the different countries and critical infrastructures? From Symantec's point of view, cyber starts to resemble signal intelligence, sabotage, electronic warfare and subversion. These can be called CY-OPs , and they are becoming more and more and never less. There are incidents that seem to be state-sponsored; other incidents that can be attributed to a single individual state. There used to be a categorization of attackers into well-meaning insiders, malicious insiders, and external hackers. The latter group includes politically motivated attacks. But these politically motivated attacks could be motivated with a wide range of political objectives, from 'I don't like my government' all the way to 'my government told me to do it'. Attribution deniability is always there, so that cyber is now linked to political tensions. Looking at places around the world that are becoming hotspots, where there are sparking political

tensions, territorial disputes, they come with cyber activity.

Israel, for example, is a very connected country according to statistics that Symantec produced in April 2013. At the same time Israel exists in a tense and politically unstable environment. This is reflected in the statistics. Israel is number two in terms of the source of cyber attacks in the Middle East. The most popular infections within Israel are malware like 'Conficker'. Therefore there is a case to be made. Protection of critical infrastructure, the government, the defense systems and the large enterprises are being discussed. But if one takes a step back, it becomes obvious that something has to be done to protect consumers, the population, the small and medium enterprises, because they are being exploited to launch cyber attacks. So the effort is about having a strategy, a plan and about being able to take the environment, the national strategy, national security strategy and bring the cyber component into it.

There cannot be a national security strategy without a strong cyber component that's what Symantec tells governments around the world. Indeed many countries are adopting cyber into their strategies, Israel being one of the countries driving this process. Some aspects need attention when adopting cyber strategies. First of all, knowing the unknown – it is known that the country will be attacked but not by whom, when, where, how. There is also always a possibility that a country's systems will be compromised. Countries therefore have to accept that they have to build their defense in such a way that they are able to withstand a hit. A popular question is whether countries are losing the arms race in cyber, the war in what the military refers to as the fifth domain. However, it is not just about the technology, it's about people process as well and therefore it is about a holistic approach to the problem. Countries and their professionals need to be bearing in mind the unique features of cyber. Things like the asymmetry that cyber has, or the deniability. In doing that acquisition of intelligence situation awareness becomes a key component, because without there is no early warning. Countries need to be prepared and capable of defending themselves, and be able to actually use the defense mechanisms. A counter cyber attack may be an option, but may not necessarily be the right answer. The question here is what kind of instruments of power a country has in place and can bring to bear in order to be able to react to the different instance. It is a nebulous world when it comes to cyber. Just because there has been a cyber attack, it does not mean there is a country behind it. And even if it is a country, it does not mean that cyber-

attacking them back will actually have any affect if they are not really connected. This makes the notion of building capability somewhat ambiguous. Clearly, a part of planning capabilities will need to be identifying the critical infrastructure and recognizing what is that that needs to be defended. Then, building the necessary level of resilience will be required.

There will be a lot of things that need to be defended but at the same time countries need to recognize that, as Fredric the Great said: "The one who defends everything defends nothing." Therefore, countries will need to prioritize.

Especially in developed economies the role of the private sector is always key, the question of how the private sector needs to work together with government in order to share information, in order to build the platforms of trust and cooperation, which would allow a better response and a better early warning as well as a better understanding of the cyber environment. There are a number of examples in this area. The US recently issued their executive order trying to push for better and more effective information sharing within the federal government. The European Union recently issued the network and information security directive trying to push at the member state level cooperation and information exchange. There is a difficult discussion right now within Brussels and it is left to see how exactly it will play out. UK, Germany, and Netherlands and number of other European countries have in place programs to work and cooperate with their private sector, and obviously NATO has in place a number of principles and mechanisms for collective defensive and crisis managing.

Cooperation in cyber is happening and it involves a private sector, which is a direction that more and more of the world going.

The other area is educating the users in the population, making sure that the community, and especially small and medium business, are aware of the risk and the challenge. From the point of view of technological requirements, the capability ultimately has to do with real-time monitoring and having a functional national surge that are able to correlate, analyze, do forensics and respond to incidents.

At a strategic level, it is common to focus on protecting the data center or the PC. However, protecting the hardware is not any longer the way to go. Now it is about protecting the information and the identities. The more common mobile devices and the cloud become, this is going to be a key requirement. Of course end points still need protection, because they are still likely to be the weakest link. Most important, however, is a risk-based

approach. A comprehensive, both redundancy and disaster recover capability needs to be in place, because eventually an attack will happen. An intelligence-centered approach is key as well, but the reality also is that the intelligence has become the default posture. Everybody is gathering data, it is piled and stored somewhere, but not enough is actually done with it. There is no point in keeping intelligence without generating knowledge and actionable items. So the challenge here is not really to gather data, but to gather data in order to classify, categorize, prioritize and analyze it in a way that will actually be meaningful. Data needs to be analyzed and categorized as incidents in order to understand what to defend against, and if possible, attribute.

So when it comes to actual defense, again, prioritization and focusing on things like containment mitigation, preventing the attacker to go any further is key. Especially when it comes to critical infrastructure operators, it is about continuity, making sure that the power is not going to go out or the server running. In order to do that real time monitoring is required, and, obviously, protecting in depths and in multiple points is needed. For example, the amount of different layers needed to defend a system from Stuxnet is impressive. Many different technologies that could block this type of attack, but at the same time – they'd need to be in place. These technologies would have to be used while working against the clock, collecting intelligence about the attacker in order to try to attribute and to understand what is the malware that is being used, what is its elementary, where it is coming from and how quickly, because it will probably be hopping around, as well as how quickly can people help you.

Any strategy will have to address organizational questions. From the experience of a NASDAQ listed company, first rule of management is have a neck to throttle, to make someone clearly responsible. In government that's a difficult thing. It is not always easy to identify who needs to be responsible, but it needs to be done. There also have to be clear rules of engagements as to what is military, what is law enforcement or what is intelligence. Also, every time there is an incident it has to be clear what is the threshold that would justify them being involved.

Very often in Europe there is a discussion about having the necessary laws, rules, regulations that will allow a country or an organization to defend itself. Quite frankly, very often in Europe there is a conflict of laws. There is a discussion about information sharing yet there is one of the strongest data protection regimes. Therefore the right balance needs to be found, between dealing

on one hand with sharing information on threats and attacks, while at the same time doing it in a data protection friendly way, guaranteeing the privacy of individuals.

Another frequent problem in the cyber space is getting the necessary skills, getting people skilled and being able to retain them. It seems, as if Israel is on the right path to educating, promoting and retaining talents.

One of the most difficult organizational questions that countries are grappling right now is building the environment of trust. How to get the people to gather around the table to share this data? It is challenging, because the subject is sensitive, tricky and involves business, economic interest, competition requirements and also liabilities. Perhaps another organizational point – regular exercises. A lot of that is done in Europe; NATO has been doing that, as do the US. Symantec as a company participates in several of those and even has an own program of exercise, because it is key. Efforts need to be put in practice to see how they are going to work. Otherwise every time an exercise delivers a good result, it does not mean it has delivered what it is actually intended to. Then, finally, when there is an incident, a cyber attack, it was managed and contained. In the end the question will be regarding the proportionate response.

This requires nations to have built a process to address things like the political, the diplomatic, the economic, potentially even the military response to attacks. The key point is again is to say that just because something happened on the cyber space, the proportionate response might not be a cyber related one. Richard Clarke mentioned what a coalition of like-minded nations can do in order to apply diplomatic, political, economic or even electronic pressure.

What about deterrence? Many people lead historically the discussions around deterrents with offensive capability, with ‘we’re going to hit them back’ and it is fair to say that whereas traditional deterrents and ‘I got a bigger gun than you’ or ‘I’ve got many more airplanes or many more tanks than you’ has historically worked well. However, when it comes to cyber these deterrent strategies are reaching their limitation. Part of this has to do with the fact that cyber attacks and cyber operations in general are claimed to be deniable and the declaratory policy has somewhat of questionable effectiveness. It is possible to show the amount of tanks or warplanes, but when it comes to cyber, showing the amount of computers in a room is not really convincing. Capability is not easy to verify and most importantly

when a country chooses to go down this path, exactly because doctrine is not yet fully developed, how should it be received by the opponent? Such a demonstration could imply a first strike, or an escalation, or an indication of de-escalation the fact the country chooses to go cyber and not kinetic, or even a preparation of an intelligence collection before a physical attack. It would raise questions regarding the hidden incentive behind the action.

This is what perhaps makes deterrence by offensive still unclear and uncharted territory to go and possibly even a difficult one. It fair to say that, certainly for Symantec, that this is the kind of challenges states are going to be facing in the coming years while at the same time that the national, regional and all capability strategies are still in development. Effective defense is likely going to prove a bigger sort of deterrent and denial to act against the presumed offensive capabilities. It is also fair to say that there is no single magical solution and certainly not a single technological solution. The approaches will very much have to customize with the regional security realties. However, as more and more militarization of cyber is happening, cyber security will more and more move in the signaling intelligence, electronic warfare and strategic warfare direction. Military system communication platforms, command and controls, are going to be target by this kind of cyber attack and the more the conflicts evolve, the more variations there will be and the wiser the professionals will become.

System Approach to Cyber Research

Mr. Doron Rotem | Director, Crisis & Emergency Management Solutions, MLM Division, Systems Missiles & Space Group, Israel Aerospace Industries Ltd.

The cyber research that I want to present isn't a purely academic research; rather it is the investigation which is a critical part in cyber incident analysis aimed at detecting harmful malware and, of course, determining how to respond. The challenge is multi-dimensional and requires a systematic approach. Organizations are seeking for ways to deal with the increasing amount of attacks or suspected attacks while they are lacking the proper resources and working within limited time frames. Therefore, they are seeking for ways to improve their investigative abilities and conduct the investigation as mechanized and automated as possible. Life for a cyber-analyst is quite difficult: there are a variety of attack vectors, ways, means, and types of malware in increasing amounts.

An abundance of malware is activated by some sort of trigger or remote activation. If the cyber-analyst tries to run the malware code, the code might not run unless the trigger is activated. So, he will attempt to deploy the code in order to build a behavioral model. Then, he will try to guess which component actually triggers the malware's payload. In many events, he won't succeed and thus the arduous process continues with repetitive menial work.

With the number of attacks increasing, there will always be fewer people than needed and not enough time to react. Can a research laboratory do the work in place of the investigators and actually replace the investigator's function in this process and instead operate automatically in order to optimize the process?

The asymmetry between the attacker and defender stems from

the fact that producing new malware does not require a lot of effort, while defense methods, primarily signature-based, are effective only in 17-40% of cases rendering the majority of work to be done manually. The challenge is how to identify harmful malware not by signature. There are a variety of statistic and mathematical methods that are not based on signature.

Situational awareness addresses the challenge of organizations today to detect attacks in their systems. It is possible for malware to persist in an organization undetected for weeks and even months. The key here is to make processes automatic. This can be achieved in a systematic approach based on an automated engine that times and synchronizes all processes: it intercepts suspicious files even in large volumes, runs a variety of analysis engines, and uses a known malware database, all automatically and repetitively. Only when there are cases that raise suspicion does the system alert a researcher to investigate. This will reduce the rates of false positives, and in the event of an actual malware accelerate the cleaning process.

We, at the Israel Aircraft Industries (IAI) have implemented this approach in the overall suite of our defenses that we've named TAME. This acronym expresses that we can't eliminate 100% of threats but we can tame, control, and curb the damage. The TAME cyber defense suite includes four main components: TAME Range-simulated cyber-attack trainer, TAME Guard-comprehensive protection suite, TAME Center- cyber command and control center, and TAME Response- cyber research lab that integrates mechanical and automated laboratory tools, which allow for malware investigation. The complete solution will consist of all of these layers thus making a full suite. The method is modular and scalable and that is one of the things we need in dealing with cyber-attacks.

Cyber Kill Chain™: Applying Intelligence to Defeat Cyber Threats

Mr. Eric M. Hutchins | Fellow and the Chief Intelligence Analyst, Lockheed Martin (LM-CIRT)

Defenders have the advantage with regard to intrusions. There is no rule of the game that says the intruder or the attacker. But the advantage of the defenders is not given for free. Intelligence is a key part of cyber security, and it is the cost that it takes for defenders to take this advantage and actually defeat persistent threats. Facing very advanced and sophisticated threats is a very humbling and educational experience. As Eugene Kaspersky says, “an attack is an opportunity to learn about the attacker” and this is where the defender could seize that advantage. Secondly, building strong partnerships and relationships with professionals is a privilege. This is key to defense, and as to collaborate as a community and information sharing is really crucial on how to learn most about the stress to the system and make the most resilient defenses.

NIST, being the National Institute of Science and Technology, operates within preparation, detection, containment and then recovery as well as post-incident activity, which can be described as an action or inter-process. These are the steps that defenders were taking, but in regard to persistent threats, defenders were never in any one step at just one time. Detecting was never finished when containment needed to start, and they were still containing when they had to detect, still cleaning up and getting ready. Incident response is a very messy process. It is very hard to say when step two is done and when step three begins.

In 2012 NIST updated this process, in a very subtle but critical way, which is to add loops between detections and actions. These loops signify finding, taking action and learning something

additional. As this continually progressed through this process this is the intelligence, this is what is learned. This resulted in an approach that is less focused on steps and more focused on the knowledge that is gained. That is how the Cyber Kill Chain® was created, which has been part of cyber security at Lockheed Martin for the past five years. Now, instead of aiming attention at the steps of defense, the focus lays on describing and understanding the steps the intruder takes. If a defender can understand the actions of their adversaries, then defenders can get intelligence on what their adversaries did and can obviously shape better mitigations and actions against these adversaries. As the name reveals, the Cyber Kill Chain was inspired by military mindset. In this mindset it is true that the intruder does not succeed unless they can actually achieve their object – a chain of steps where any broken step means that the intruder does not succeed. Many significant players, such as TrendMicro, Dell Secure Works, RSA and even Facebook, are talking about incorporating this analysis framework into the protection of their networks and the course of their research.

The first step is reconnaissance – how to select the target that they want to engage. Most of the APT intrusions are socially engineered, therefore the process principally begins with selecting email addresses. This may happen via a Google or a social network search, it might be looking for press releases, contract awards or conference websites that are always a good source of information. This is the first step for how to figure out whom to target. The next step – weaponization – is one of the most crucial steps in that it describes how the adversary generates malware. Do we most adversaries write malware by hand? The answer is no, most of them use it as a tool. The probably most well-recognized tool is Metasploit. There the adversary can pick an exploit, the payload and by clicking on ‘generate’- create a malware. The problem for the attacker is, however, is that if they do not know all the fingerprints that Metasploit leaves, they might not realize that they are being blocked all the way by the defenders. What this example shows is also a supply chain to the adversary. The adversary has places that they procured by or download tools and then the defenders can see which adversaries used the same tools, which tools are public, which tools are private and which adversaries have their own tool makers. These are very critical pieces of intelligence and important for how defenders can mitigate these intrusions. The third step is delivery – how the malware is sent to the target. In most cases, as mentioned earlier, social engineering

is very common, making email the primary method. There is also an increasing trend of the so-called watering holes websites. By compromising a particular website, the adversary is targeting a particular audience. Additionally there are, of course, also cases of server-based intrusion attempts, possibly with web protocol HTTP as the delivery mechanism. The forth step is exploitation, or how the adversary gets control within inside the environment. It might be software or hardware vulnerability. The whole point is how to allow the malware to execute inside the environments. The fifth step is installation – if the adversary wants to maintain persistence inside the environment, they must set up a system that will continue to make the malware reboot, for example. It might install as a service or an autorun key in a Windows registry. The sixth one is command and control – a way for the attacker to communicate with the malware. Once the malware is inside a network it also has to get out. Most networks everywhere allow web HTTP out of the network or it protocol like DNS or maybe even email but how does a malware get out? Then there is the last step of actions or objectives, what do the attackers actually seek to achieve? Commonly in persistent threats malware is not automated, but purely a means to expose access. What happens next depends on whose hands are on the keyboard therefore the seventh step is left very open. It also depends on the objectives of the threat – is the objective destructive or is it an objective to steal information – so that what may happen in the very same step, step seven, might differ from between stealing data versus destroying data or sabotaging three thousand systems. Understanding what might happen in step seven is critical to prioritizing the analysis, and that is how defenders can track the campaigns.

There is the Kill Chain and the most important thing is that any mitigation breaks that chain. Even the most sophisticated intrusions can be stopped in one spot. Often professionals say that the attackers have to be right just once but the defenders have to be right every single time, but possibly it is the other way around, a defender can be right just once and break intrusion. The attacker has to be right every single time to achieve their object and that should be the call to all defenders to seize that advantage, rather than hang heads and say that it is impossible to be perfect.

At Lockheed Martin this approach is used in seven ways. First and foremost, sensor alerts are prioritized. A lot of money is spent on a variety of tools and one might wonder which tool to analyze first. However the point is not about the tools, the point is about

what notifies of the intrusion. The later, the sensor alerts of the kill chain the faster defenders want to respond. This makes a very clear prioritization of eventuation analyze. Therefore, the key step is to take all the alerts from vendors and the own, customized rules and tag them based on what kill chain step they indicate. Kill chain step seven requires immediate attention, while kill chain step one alert can be dealt with later.

Second is escalation, which is an example of how the cyber kill chain is a tool that helps both analysts and leaders. There are four different points of escalation and that an intrusion that gets past step three is called call delivered, and that has to get notified to the server manager. An intrusion that gets past step five causes a compromise and it goes to the management above, the director. If the intrusion surpasses step six it is labeled unshielded, meaning the intruder is all the way in the system and there was no mitigation to block the intrusion back out, but the intruder may not have had impact yet. At step seven the CEO is notified. In this way there is a very clear model to articulate an intrusion based on its progress.

Third – how to prioritize investment. Again, understanding for the ways in which an adversary is operating allows for tailoring and developing the right mitigation to stop them. Different courses of action can be chosen for different purposes, for example based on the five D's: detect, deny, disrupt, degrade and deceive. Also, each action will yield a different result. If the adversary is following a tactic that the defender has no mitigation for, then this is the place to invest. What it also shows is that it is not just about the big vendor tools, it is also about the users. Employees are a very key investment at Lockheed Martin, which rigorously trains all of its employees. They might get a test message - three thousand a month are tested this way. Intrusions that are results of employee mistake are on the rise, therefore it is a very important investment and, in this case, a great delivery detection mechanism. Different methods fit inside this framework. The point being that planning allows for more effectiveness in execution.

Fourth – effectiveness, as the opposite of the previously mentioned priority. The earlier an intrusion is blocked, the more effective are the defender, which is a very powerful way to measure different intrusions and effectiveness in containing them based on early detection. As defenders start to track campaigns and intrusions over time, it is possible to say whether it is the defenders or the adversaries getting better. At that point also the tradeoff of intelligence will be visible – of who is learning more about whom. The fifth way is measuring resilience. Resilience is a key element

of defense against persistent threats and can be illustrated with the following four cases. The first one was blocked at the delivery, which was good, but there was not any other mitigation waiting after the facts. The second one was blocked in installation, step five, but there were also two other mitigations at six and seven that would have stopped it if the intrusion had progressed that far. In other words the second system was more resilient in the second one. Again, of all the intrusions that a defender is facing, the action that might need to be taken next is focused not on blocking three and four for the second intrusion, but figuring out what mitigations to add resilience at four, five, six and seven. This is how resilience is built.

Adversaries are going to change, but if there are other mitigations waiting, one mitigation still can beat them. What it also shows that even when intrusions are blocked there is still analysis to figure out what would happen next. So this is actually a very key distinction of an organization that is intelligence driven. If, for example, a virus scanner blocked a malicious PDF file, the job is not done, and so defenders go ahead and analyze things that have been blocked. Many people will say it is blocked, the risk is mitigated, but an intelligence-driven organization will seize the possibility to something new that will help protect it against an intrusion tomorrow.

And the way to collect that data is to fully analyze an intrusion forwards and backwards, measure how far forward or backwards the attack can be explained and the last one, and very crucial, is tracking campaigns. When intrusions overlap there are commonalities and patterns. This way defenders can trend campaign overtime, and act proactively. They can start to anticipate when the next attack would happen, and measure their effectiveness against the campaign. The millions and billions of malware that are discussed nowadays are probably the result of forty, fifty, maybe sixty different campaigns. It is much easier to understand one's own results against fifty campaigns than against a billion different packets. That is what should be measured and that is how intelligence can be applied, driving the right kind of action. And so the framework presented here, the cyber kill chain, is a mean to explain how the defenders have the advantage, how defenders can learn about the adversaries, apply that intelligence and achieve true resilience.

03

Third Session: Cyber Technology: The Next Generation

Singapore's Approach to Cyber Security

Lim Chuan Poh | Chairman, National Infocomm Security Committee (NISC) and Chairman, Agency for Science, Technology and Research (A*STAR), Singapore

The particular topic of cyber security is a topic that is still emerging and therefore there is a lot that countries can do to share with each other and also to learn from each other. The rapid advances in the info-comp technology have brought about some profound changes to societies and economies. These changes are continuing as more people are participating in cyber space. By the end of this year, ITU estimates that a number of individuals using the Internet will reach 2.7 billion people and mobile broadband penetration will see 2 billion. A part of this increased reach, ICT has transformed the way people work, live and play. Global e-commerce sales reach US\$ five hundred seventy billion, in 2010 and went up to US\$ eight hundred and twenty billion dollars just in two years in the year 2012. It is also predicted that worldwide e-commerce sales will reach nearly US one trillion dollars this year.

As a subset of e-commerce, mobile commerce or m-commerce is also expected to follow in the very same steep growth. Another report estimates that global mobile payment transactions would generate US\$ 240 billion dollars in 2013 and this will increase threefold to US\$ 720 billion dollars by the year 2017. According

to this report, much of the growth will come from three countries: South Korea, Singapore and India.

ICT has also changed the way people socialize. Like in many other countries, ICT and the internet have transformed Singapore. The percent of the population who use the internet more than doubled from thirty six percent in 2000 to over seventy five percent in 2010 and growing. ICT is now an integral part of life in Singapore. The Singapore government has played an important role in facilitating this shift in the society. In 2007 the government launched the wireless at Singapore program that offers three wireless broadband accesses in almost all public places. In 2008 building of the nationwide fiber optics broadband started. By middle of 2012 Singapore has installed fiber optics in 95 percent of the homes and offices, the rollout was planned to be completed in 2013. These investments in turn have capitalized the Internet service providers to offer more broadband to users at very affordable prices.

Apart from the infrastructure development, the Singapore government is also one of the early advocates of offering e-services to the people. The first e-government action plans were launched in 2000 and since then more than 1700 applications are available online. Based on annual user survey, acceptance and use of these online governments services have grown over the years. For example, the proportion of taxpayers who e-filed their tax returns grew from 30 percent in 2000 to nearly a hundred percent in 2013. These high participation rates are not unusual for many of the other e-services. Of course it helps in the case of Singapore, to have very simple tax rules and a much lower tax rates compared to many other jurisdictions. In Singapore, e-commerce sales reach 1.1 billion Singapore dollars in 2010 on nearly 4 percent of the total retail sales for that year. Two years later it climbed to 3.1 billion, and this is expected to reach 4.4 billion this year. ICT direct contribution to the Singapore economy has also been rising steadily since 2005, when the total info-com industry revenue was 38 billion dollars from hardware, software, telecommunications, IT and contents services. The industry has shown stable growth and reached over 83 billion dollars in 2011. Moving forward, mobile Internet use is becoming further entrenched as the preferred mode of accessing the Internet. In Singapore, mobile commerce saw a dramatic eightfold jump from 40 million dollars in 2010 ago to 330 million dollars in 2011. PayPal predicted that m-commerce will grow tenfold to reach 3.1 billion dollars in Singapore in two-year's time. To align themselves

with this shift the three main mobile operators have already rolled out near few communications last August for 20 thousand payment points right across the island. The government has also launched the mobile government app in 2012, to facilitate use of the government services by the population.

The breadth and depth of ICT's reach have left very few facets of life untouched in Singapore. Unfortunately, this ubiquity also means that cyber space has now become a very lucrative target for attacks. Being an open and highly connected economy, very similar to Israel, Singapore is obviously not immune from these attacks and has to take appropriate measures to respond to all these threats. To deal with the broad nature of cyber threats and recognizing the limited resources of any single entity, Singapore has always emphasized the need for collaboration both domestically with internal state orders as internationally with counterparts overseas.

In Singapore the government maintains oversight and policy coordination through a high- level committee created to formulate the national cyber security strategies. The National Info-Com Security Committee, or NISC, was established in 1997 as a key decision body to set in full communications security policies and strategy direction at a national level. The membership is drawn from many different agencies, and it is a platform that is intended to balance economic development with national security considerations. Balance is needed between both, the desire to grow the economy and of course the security of the country. The committee also provides the guidance for a national cyber security strategy and it is capsulated in master plans. The first master plan was applicable from 2005 to 2007 and primarily focused on leveling up the capabilities of the public sector to deal with cyber threats. A cyber watch center was set up – one of the first in Asia to provide around the clock warnings on cyber threats to critical installations in public sector. To compliment this detection capability, also a threat analysis center was established to gain a better understanding of what needs to be contained. Aside from the public sector, efforts to protect the info-com system and critical infrastructures were initiated under the critical info-com infrastructure security assessment framework. This was intended to ascertain the readiness and adequacy of the protection measures implemented by infrastructure owners and operators and most that are mainly from the private sector. In 2008 Singapore adopted the second master plan to maintain the protection of the public sector welfare during the efforts on the

critical info-com infrastructure. Recognizing the unique needs of each critical sector where there is energy, info-com, finance or the transport sector, the government works with critical infrastructure owners to assess and develop sector specific info-com security requirements.

One such program is a secure and resilient Internet infrastructure practice. It was issued in February of 2011 for the Internet service providers. The code covers the protection of the core Internet infrastructure, such as routers, switches and critical network components, and states objectives and controls necessary to prevent, detect and respond to the cyber security incidents. The code also allows the ISP and the info-com development authority to make more informed decisions, so that early warning to emerging cyber threats can be developed and the appropriate preventive measures can be taken. For the ISPs implementing measures need to be consistent with international standards and best practices. This enabled them to better protect business and consumers against cyber attacks. In this second master plan also programs were started to boost the IT security work force. Working the private section an association of info-com security professionals was set up to transform info-com security into a distinctive profession and build a critical pool of info-com security professionals in Singapore. To boost the number of such professionals, a national info-com scholarship was launched in 2008 to draw talent into this particular sector. This scholarship has since been expanded to generate even more talent for the sector.

The prevalence of Internet use among Singaporeans does not automatically translate into IT security awareness or best practice. To raise awareness and adoption of essential cyber security practices among the users, cyber security awareness alliance was created, engaging partners from both public, private and also the people sector. The alliance aims to engage the people sector and empower them with resources to stay secure online. It does initiate various collaborations and programs for the different segments of the populations from young students in the school to working adults. Internationally Singapore is also an active participant in the global efforts to address cyber threats. In 2008 the working group on international collaboration on critical infrastructure protection, or ICONIP, was launched. Singapore leads this working group with members that include Australia, Japan, the Netherlands, UK, US, and the ITU. ICONIP aims to provide government worldwide with the means to exchange ideas and initiate actions for cooperation

on critical info-com infrastructure protection. One outcome of ICONIP's collaborative was the development of a self-assessment scorecard on critical Infocomm infrastructure protection. Finalized towards the end of 2009, this scorecard is self-service tool for the CI owners, operators and regulators to monitor the security preparedness of the CI on a continuous basis. It also serves as common assessment tool of CI security health or readiness in an organization or across an entire sector. Singapore's commitment to transnational cyber security collaboration is also evident in the regular exchange of information and experiences in regional forums such as the Asian telecommunications and IT ministers meeting and also the Asia Pacific Cert.

Singapore has made substantial progress towards the protection of the government and also the critical Infocomm infrastructures. However, one area in which the country faces a challenge is education – persuading small businesses and the general user to internalize cyber security practices, but Singapore continues to work on this. The country will continue to reinforce efforts on securing the government and critical Infocomm infrastructures while broadening the scope to include the smaller businesses that make up the supply chain, as well as individual users who form the broad base of the information system.

Given the rapid evolution of Infocomm technology and threats, Singapore recognizes that it is insufficient to rely solely on off-the-shelf solutions. The Singapore government has been investing in Infocomm spending on average of one billion dollars every year. At the same time, the research has produced some encouraging results so far. This includes developing the lightweight cryptography that was adopted by ISO as an international standard for detection software that was developed for Visa International and a smart grid security framework developed for charging electric vehicles.

The country wants to build on this progress to do more and to cultivate an even more conducive environment for research and innovation, recognizing the academia's push for breakthrough discovery, the industry's goal to constantly find marketable solutions and the government's desire to secure the cyber space for both business and society. There is a need to explore new frameworks and funding schemes to stimulate more meaningful and impactful research collaboration between public and private, and also between public and public organizations, while ensuring that the most deserving solutions get funded. Singapore also is looking into continued cooperation with its international partners to build collaborations and Israel is in focus for meaningful

collaborations. In conclusion, to deal with the dynamic changes of the cyber landscape Singapore fosters and maintains close partnerships among public, private and also the people sector to boost a cyber security capability of each of these sectors through a coordinating approach. At the same time, along this journey Singapore believes that collaboration and partnership provide the key.

Panel Discussion:

Mr. Eli Yitzhaki | Strategic & Business Development Leader,
ELTA SIGINT EW & Communication Division

In spite of thinking in revolutionary terms and a whole new area, cyber security is one element in ongoing information warfare, and not necessarily a whole new type of warfare. There are a few critical elements for security like encryption, compression and distrust in foreign elements, they all refer to modern systems, but also to the info-com. The system needs all those elements.

In a historical perspective, throughout the evolution from carrier pigeons through the telegraph, radio to data links, the Internet, denial of service techniques, and are, used – from falcons to hunt carrier pigeons, cutting wire in the telegraph area, jamming electronic information from Morse radio to radar to the today's infamous DDoS attacks. Neither have the intel elements of deciphering codes started with the internet - the era of carrier pigeons also brought about encryption and decryption. Later on elements like COMINT and ELINT became very important tools in intelligence gathering, in a more general term, signal intelligence. It is still there and it has a lot of resemblance to the cyber domain. False information, either replacing notes on the pigeons, rerouting wires and sending false telegraph information or send false information via Morse. Other methods, like false information in the radar are very famous and known as spoofing, either coherent or non-coherent. Signal intelligence is part of any military security activity in today's era. What is important is to look at the means for accessibility into the domain from hunters during the pigeon era, wire hacking is part of the capability to hack into telegraph during the civil war in America or radio hacking, which provides all the capabilities to either listen or interfere with radio communication.

The fairly new accessibilities are techniques of computer hacking. These are different, but still use a lot of the old tricks. Counter measures, which also constitute security measures in this context, started with speed and multiplications of elements during the pigeon era, encryption in case of the information falling into the wrong hands. During the telegraph wire dominance, those who dominated the wire could ensure the safety of the message. Today it is mainly firewalls, anti-viruses alongside with some capabilities in encryption on the Internet and more complex things that exist with the RF networks. When discussing radios, it is worth mentioning that there are many capabilities within that reduce the probability of interception distance for Low-Probability-of-Intercept (LPI), frequency hopping and other techniques.

All those exist, thus today there is a new domain, but not a new subject. It is the same old subject with a new domain that has advanced and gained importance. The question is what cyber security is, and the answer appears to be in the move from perimeter security to defense in depth, which means in security to move from trenches and semi-fixed obstacles, such as firewalls and antivirus, to predictive dynamic intelligence-based situational awareness including action-indicative signs and timely alerts to initiate adaptive, changing security measures. In other words, the attackers should see a different response at any given time, even if they repeat what they do many times, creating a difficulty to predict the weaker points of the defense. This change primarily has four requirements. One of them is to be able to model the cyber environment using tools for scientific modeling of complex entities and the relationship between them. This is necessary to better understand and predict system behavior. Another element consists of mathematical fusion tools, served for fusion of radars, electronic warfare and SIGINT, which are all massive data packages. The third is operational erase tool to optimize the security activity, which is needed to be able to apply the best defense against a problem identified though situational awareness. The last necessity is computer hacking know-how.

Mr. Avi Chesla | Chief Technology Officer, Radware

It is pretty obvious that lately the financial sector has gained significance as an attack vector. A campaign of significant attacks was launched against the financial sector in the US in late 2012 through the beginning of 2013. More general attacks started somewhere in 2010 with the Anonymous attacking PayPal, MasterCard, Visa and further on to government and to the international financial sector. Almost every stock exchange in the world was under attack – the Hong Kong exchange, the New York Stock Exchange, the Toronto Stock Exchange and others. In terms of DDoS, since 2012 the attack durations have significantly increased from a few seconds or minutes to lasting several hours, days or even weeks. Some of the longer lasting attacks on banks continue for over a month. This dramatically changes the behavior of the organization, which means it that the attack is not limited, and requires advanced skills to fight, which many organizations are unlikely to have. Another angle of the complexity of attack is the diverse application or the multiple vectors of attack. Usually attacks are coming simultaneously against the data center. There is a new level of complexity to attacks in terms of duration, diversity and dynamic nature of attacks, the number of targets in a single attack at the same time, creating a trend especially in the DDoS area. This results in concerns regarding not only technology, but also the lack of experience on the market. Most organizations are very skilled in preparation before the attack, which includes policies and some investigation and forensics for post-attack analysis. At the same time, skills needed during the attack become more significant. Because attacks now last not minutes but days or weeks, there are new requirements for an emergency response that fights and resists these types of attacks. One of the new techniques is an ERT that has the capability to create a counter attack – the main idea is that once there is an attack in order to try to not only block it, but also make the attacker quit, the response needs to attack them back or to neutralize the resources they can use to analyze their target. This will eliminate the benefit of continuing to attack the same target, making the attacker move on to another target. The technology involved in such response is the capability to monitor the traffic in real time, to search for patterns of known attacks tools or even new tools. With help of dynamic patterns, it is possible to find and analyze operation limitations in these tools, such as computer operation

limitations or design operation limitations. Once a discovery is made, it is possible to slow down these tools, attack back in the same matter, and it is possible to do so successfully. Not in all cases, but in 10-20% of the cases, it is possible to create these counter attacks resulting in attackers giving up and moving on to another target. It is the skill of counterattacks that still needs to be developed.

Another technique, which is completely different, is a new networking network, the software defined networking (SDN), which provides a new opportunity to have a security-aware network. Companies or organization that have not yet invested in analysis and research of this area should start to do so, because SDN allows not just hosting the firewall and the antivirus or specific security services, but also enables the network to be part of the monitoring, the detection and to be part of the defense, the protection, and the blocking tool. Software defined networking in general decouples the control from the networking forwarding in the network fabric and brings it up as a centralized control layer. This layer is the network controller, and the opportunity to create new applications on top of this controller, which also includes security applications. Through this security application, the network can not only be configured but programmed to change the behavior and to be able to be part of the security framework, not just host it.

Tal Mozes | Hacktics Leader, Advisory Services, Ernst & Young

In contrast to what might seem like common sense, innovation and invention appear predominantly in cyber-attacks but not as much in defense technology development. All along, innovative defense concepts and the development of products have been done primarily in the private sector and less in the government sector. Looking at this from a purely technological perspective, new technologies emerge and advance, but at the same time, progress that was achieved often regresses and security breaches that have already been corrected appear in new releases. For example, Bluetooth version 4 has certain vulnerabilities that existed in version 1 but were fixed in later versions. Another interesting example is that of LTE, proving that no lessons were learned regarding the information security breaches that we are already familiar with from the (soon to be) legacy GSM protocols. How did this situation come about? The regulations are unable to catch up with the technological gaps and can't properly address cyber-attacks and the new sophisticated enemies that we see in the world today. The same can be said for the regulation of SEC of companies traded in the American stock exchanges, which mandates cyber incident reports, but fails to address the topic of cyber and offer a complete solution. Today, the United Nations oversees trade in unconventional weapons, but what about in the cyber world?

Still today, most of the cyber security resources are directed at developing targeted attack abilities and intelligence gathering but not at the development of cyber defense mechanisms. Both the public and private sectors rely mainly on off-the-shelf products for identifying and preventing attacks. The defense's effectiveness is relatively low because the same off-the-shelf products are being used everywhere. Yet, there are those who have stronger methodologies, better separation of networks, and better configuration, though it is still using the same products with the same activities. There is a genuine need for a shift in approach. What should be changed? Most of the attacks that we come to learn about through the media are actually the unsuccessful ones. Stuxnet failed in that it was exposed. The successful attacks are those that continue to operate in stealth, meaning that no one actually knows how many successful attacks are currently operating in the world as we speak. Every organization must assume that they will be the target of a cyber-attack in the near

future or that they have already been attacked and hit. Therefore, we need to be proactive and monitor endpoints and servers in the organization in order to collect intelligence. We must raise awareness at all levels, not just at the low or medium level, but at the top executive level. We need to perfect the regulations and enforce it so that it can address current and relevant threats. For example, PCI, which regulates credit card companies, not by governments but by industry, is successful in that it imposes a hefty fine on entities that do not meet the regulations.

A good example from Holland is a botnet by the name of Bredolab, which infected the computers of tens of millions of users. The Holland Police connected to the computers of those who were affected and initiated treatment. In doing so, did the police break the law or did they provide a loyal service to their citizens? This is a legal issue but it's definitely an interesting precedent.

Ernst and Young alone has 3,600 information security consultants spread worldwide, which is quite a large unit with a great deal of knowledge. These minds can be leveraged to contribute to the protection of any state.

BG (Ret.) Yair Cohen | Head of Cyber Security, Elbit Systems

Winston Churchill is attributed the phrase that after the First World War the world understood that the air dimension will be crucial during the next war, but just not how much. The same equation is relevant to the cyber domain. It is acknowledged that cyber will be crucial in the next war, but just how much crucial it will be is not yet understood. Currently there are probably five hundred million attacks happening every second. This assumption is based on CheckPoint's assessed three hundred million cyber attacks against their infrastructure in 2011.

Barack Obama and former US Secretary of Defense Panetta stated that the military and the civilian sector are under constant attack. Estonia in 2007 and Georgia war in 2008 showed what happens in war by cyber.

The most interesting cyber attack that has occurred was Stuxnet in Iran. For the first time a physical cyber attack was conducted. The important aspect of this attack is that attackers have found a network where ninety percent of the whole infrastructure, also in Israel, is based upon SCADA, which in turn is based upon protocols from the 70's and the 80's. Therefore there is a crucial need to find a real solution to safeguard SCADA systems of all critical infrastructures

There are challenges in the new battlefield. There is no real solution to identify the attackers. But even that is not enough, a certain level of preparation and a certain level of intelligence gathering are needed – before the systems are compromised. Once the attacker succeeded in planting a Trojan horse - it is too late. Therefore the real challenge is to identify the real attacker while he is still in the stage of preparations. Arguably, cyber brings an asymmetric component to the table and from the intelligence point of view, in the everlasting game between the attacker and defender, there is a huge gap is generated in favor of the attacker. "We built our systems upon capabilities that we have not learned how to protect," said the former head of the CIA and NSA.

There is also something very crucial given the experience in the cyber world so far, cyber allows for the first time to cause physical damage in what is called cease fire, in peace time, because an attack can be launched without being accused for violating the cease fire. To exemplify it with the situation between Israel and Hamas, There is temporary cease fire, and no side, based the common interest, would like to attack each other except in

cyber, for example to gather intelligence. Many operations can be conducted which would be classified as offensive, without being accused of violating the cease fire, which creates the temptation to do it.

The great Israeli poet Yehuda Amichai said that “there is permanent war in the world, but all the time it is in another location.” Another saying tells that peace is actually war and war actually peace – something that describes the situation around cyber so far. Globally, actors try to prevent attacks upon their IT infrastructure, but it is not enough. A proactive approach is needed; the attacker needs to be found – before he enters the networks. This is the solution, because although they will be crucial building blocks in each cyber protection, security devices are not sufficient. What is needed is a center that can deliver intelligence, in any country, military or large organization. This intelligence gathering in cyber is not SIGINT or ELINT. It is a new kind of expertise that has the ability to see the attacker. It requires whole information and is similar to the intelligence world. The information has then to be stored and analyzed, finding anomalies, creating situational awareness. It is a challenging and costly venture, but it needs to be implemented. There is also a need for clever regulation and enforcement and to adopt something like the sensor to shooter cycle. The world of cyber has brought about something yet unknown, it is the same but different, and it needs to be addressed.

Andrey Dulkan | Director of Cyber Innovation, Cyber-Ark

Cyber Ark is a global cyber security company, a recognized market leader, with over thirteen hundred enterprise customers, including leading companies and vectors such as energy, banking, defense, pharmaceuticals and many others. Naturally, the company also engages in technological research.

In a coordinated attack in December 2012, a group of hackers breached into an Indian bank, elevated the withdrawal limits on accounts and then throughout twenty six countries they withdrew money from ATM's to the sum of five million dollars. In February, two months later, they repeated this action, but with a credit card processor, to withdraw forty million dollars. In total they stole forty five million dollars. In March 2013 the networks of three major South Korean banks were paralyzed, as well as networks of three media companies and an official investigation showed later that it was a North Korean attack, motivated by political reasons. In December 2012 the New York Times and the Washington Post revealed that they have been breached and the goal of the attackers was to recover information about journalists who were investigating corruption allegations in the Chinese government and their sources.

What distinguishes these attacks is that they are all targeted attacks. They target specific organizations and they are not opportunistic. The attackers are funded and directed by criminal competitor or government elements. They collect mission intelligence on the specific target that they are after. They will use various attack vectors and if one vector fails, they will try another until they succeed and usually they prefer a low and slow approach.

Recently there were many attacks directed at destructive goals, for example the attack on the Saudi company, Aramco, where thirty thousand machines were destroyed and hard drives deleted. There is a joke about two hikers who are hiking through the forest when suddenly a huge brown bear appears. One of the hikers drops his backpack and starts lacing on running shoes. "What are you doing?" asked the other one, "you won't be able to outrun the bear". "I don't need to outrun the bear; I just need to outrun you". This is a good analogy for opportunistic attacks. When the attacker is going after personal information or credit card number it doesn't matter who the target is, having better security than the next guy will keep the first one protected. But with targeted

attacks, the bear has a definitive target. Analyzing these attack, perimeter breaches can be identified – easier and easier to achieve since the attacker has unlimited tries. He has thousands and tens of thousands of potential goals, all the company employees, and he will eventually succeed in installing a breach in the organization, meaning taking over a single land point, for example. The last stages of course the attack will be achieved. All the leading organizations today, operate under the assumption that they have already been breached and that the attacker is inside. The fact that the attacker is inside does not mean that the attacker has achieved his goal. It only means that the attacker has compromised an endpoint or a mobile device or any other means through which he will operate. What the attackers do then is that they exploit privileges of administrative or application accounts, such as root on Unix, because these accounts' privileges allow hackers a high permission for operations, which they need in in order to achieve their goals.

For example, an SAP application that needs to access its database will have a connection stream right where the credentials are hard corded. If the attacker has a particular target, he knows what users have the privileges to access this specific information and social networking accounts. These are not in the same category as privileged attacks, but the kind of damage an attack on the Twitter or Facebook account of a major operation can do once hijacked is still considerable.

In a simple attack, once the attacker is inside the network he extracts the hashes from the active directory and then he operated as a legitimate administrator with legitimate administrator tools. In another attack, the attack on the South Korean infrastructure, the malware propagated from Windows machines to Linux machines. It did so by looking for hard corded credentials that resided in remote access applications on the Windows machine and just took those credentials to access the Linux servers. Another attack came from a service provider whereas the goal was the company. When they blocked that attack, the attacker went after a business company A and tried to infiltrate company B through them.

The solution proposed consists of three steps: protect, detect and respond. First of all, protection is putting a central system in place, which will control all the privileged access. It replaces the access credentials to all organizational assets and from that moment onward users, applications and business users will all perform all of their privileged activity through that central center. This enables control, management and monitoring of all the privileged actions.

The second step is to analyze all of these actions, in order to build a behavioral profile over the attacker, understand what is normal and what is an abnormal. It is very difficult to do that without that central system, because the attacker will operate anywhere in the network and a huge number of sensors would be required. With the central system everything that is happening can be analyzed. The last step is, of course to respond. This can be done through the security operation center of the company or if there is a central system in place, the malicious activity can be terminated directly, which is a huge benefit for any response. To sum it all up, target attacks are going after privileged accounts since they want to exploit them, to impersonate privileged users and to operate in the network. This could be mitigated in one solution by protection, which means installing a central system, detecting abnormal activities, which can indicate illegitimate use of these credentials, and response, either by terminating those malicious sessions or through the established procedures of the security operation center.

04

Fourth Session: Hacking the Human Brain

Brainihack: How neuroscience can inform hacking and vice-versa

Dr. Moran Cerf | Neuroscientist, UCLA and NYU
and ex-security expert

Francis Crick is probably known to many as the person who won the Nobel Prize in 1953 for cracking the code of the DNA along with James Watson. He took a sequence of letters: A, G, C, T, found the meaning in them and wrote a beautiful paper that suggests that life can be explained using those simple characteristics.

What is less known about Francis Crick is that before his career as a biologist, he had an upbringing as a hacker. He spent a lot of time working for the military in the 1940's trying to break codes and find ways to use information coming from signals to give meaning to potential attacks. A few years before he died in 2004, he expressed his fascination for the fact that there are still hackers doing the same work that he did sixty years before, and gave the idea that maybe someone should think about using the same methods that are used for hacking computers to hacking the ultimate machine, the brain.

There is indeed something to this statement – the brain is like a black box, where humans control the inputs and see the outputs, but still do not know what is going on inside. The same methods are sometimes used in completely different areas and so hackers and security professionals can learn from looking at the brain and vice versa. In the brain there are networks of cells, communicating

between each other. There is also a vast level of complexity there, cannot be apprehended just by looking inside. There are neuroscientists who use external methods to look at the brain – they observe the magnetic field inside, examine the surface using EEG, but the ultimate way to study the brain is to put a microphone right by its cells and listen to them speak. But for that we have to do something pretty invasive. In order to do so, however, a very invasive procedure is necessary because it requires opening the brain and inserting something into it. While this is often done on animals, few people would let researchers open their brains and look inside, other than people with brain disorders that require brain surgery. These people allow neurosurgeons to expose the brain and put electrodes deep inside trying to study the malfunctions there. The idea is to put electrodes inside and to monitor the brain over a few days, until it is clear exactly what part of the brain is malfunctioning. But there is something else that can be done with such procedures. The electrodes can be used to study the brain from the inside – asking the person a question and observing what parts of their brain lights up. Putting electrodes into someone's brain allows scientists to read things that otherwise are not accessible.

Reading and understanding the brain allows researchers to seek new solutions, to even see and decipher thoughts in action before they even get verbalized or even project the thoughts in front of the patients' eyes. Also, something entirely different can be done – those thoughts can be connected to a machine, a machine that is operated directly from the brain.

It is also possible to reverse this connection and activate someone's brain. There is a small algae that is well known among scientists, because of the unique cells on its surface that respond to light by becoming active and effectively releasing positive ions. While this activity itself might be harmless in an algae, the function can be used for example by attaching the DNA of this algae to a virus and giving this virus to a person, where it attaches to the unique individual brain cell rendering this cell active by light. Shining a light on that person's cell would activate that particular cell and make this cell go live, also following by action.

There are cells that control motor movements and cells that control other things, like making someone fall asleep or wake up, operable outside the brain by machines. This is so far done only in animal experiments, but the theory and technology to do the same with humans are in place.

So far, this covers the brain as a machine that just reads output,

reads or writes information, but is it possible to predict information? Is it possible to learn patterns of behavior and to react to actions before they are even thought about?

Is it possible to even reverse this and let the unconscious inform the world outside? A researcher group in Stanford tries to use information from the brain, from the unconscious, to create a security device. This is how it works: It is well known that there are processes in the brain that happen behind the scenes, in the unconsciousness. This group created a simple game to train and use these processes. In this game, circles are falling from above onto corresponding buttons labeled with letters. The persons were asked to quickly press the buttons to keep these circles from falling for about five minutes. What they did not know was that this sequence of about thirty letters repeats itself again throughout the game. They became better and better throughout the game. Although they would not remember the sequence of the letters they pressed, somehow implicitly their brain learned it, their muscle memory was now aware of that sequence and they, subconsciously, became better at predicting the sequence. With this knowledge, such a sequence could be used as a key to a nuclear plant. If ten people were selected, but only one trained, he or she would become better in predicting this sequence and then use that as a key to the nuclear plant. When they would come to the door, all the ten people would be asked to play the same game. The one person actually trained to be good in the sequence for about twenty-four hours, later is able to use his information to open the door much faster. Because he or she has learned using this implicit information, he or she can open the door.

Vision is the very powerful mechanism in the brain; it allows us to process things really fast. For example there is Captcha, which uses vision to stop spammers by making it hard for to create accounts without having vision. But vision can do even more. When the US Navy SEAL team 6 penetrated Bin Laden's compound, they killed him but also collected a lot of information that was later used as intelligence material, within an hour. They collected DVDs, computers and tapes, trying to take as much as they could. But how did they know what to take since they could not take everything? They took whatever they saw and they tried to assess whether it was valuable or not. Presumably, if a hard drive is encrypted, there it is more valuable, than if it is not, but how would one know whether it is encrypted in the first place? It turns out that vision is very good at assessing, whether a hard drive is encrypted or not. A hard drive that is encrypted looks

much more random and the human eye is very good at identifying patterns.

Connecting the brain to machines takes information on what the brain does really fast and uses it. Even other parts of bodies can be connected to machines. In the US about sixty thousand people have their pacemakers connected to computers and with IPv6 there's going to be endless amount of more. There are also insulin devices connected to the computer and now also brains. A prosthetic arm can be operated mostly by the muscles in the body but also via an iPhone app that was developed by Digital Eye. This App is available on AppStore, free of charge, and automatically allows remote control over the arm.

A long time ago, criminals were wearing gloves and masks while breaking into banks. This is now translating into people who are using different tools and techniques that are inferring how hacking was done, but using them for something else. Crick, who tried to use his knowledge to make the world better in understanding how the brain works, is actually the founder of this that is now looming, the most intrusive type of attack those hackers are now at, bio-hacking. Things that use biology as a mechanism to cause harm and damage, so the irony is that looking from the hacking point of view to the scientific full of view there is a full circle to how information about brain can be used to do a better job in preventing attacks.

Towards HOMO SAPIENS 2.0

Mr. Yanki Margalit | Social entrepreneur, Chairman SpaceLL,
Partner Innodo Ventures

Let's observe today's occurrences and attempt to think together where this will take us in the future. Our story is that of two heroes. The first being silicon and the second is carbon. First, silicon is becoming ever more intelligent. Personally, I think that computers can think. I am familiar with the theory that computers don't think, but they do, in a different way though. Silicon is getting smarter, that much is evident.

Secondly, carbon is hacked. The previous presenter (Dr. Moran Cerf) presented the best example for carbon is hacked; starting from the molecule level, through the cell, organism, person, and all the way to the whole of mankind. We can create interfaces between carbon and silicon.

Connectivity is improving and in the Internet of Things some of the "things" are already carbon, some are silicon, and they are all evolving mutually. I will now present ten stories on silicon and carbon. The first story is that of Watson, a computer that became the world champion of "Jeopardy." The architects of this computer, from IBM, are saying that in the next stage Watson will be assisting doctors in making decisions. Of course, they're being politically correct and what they actually intended to say was that this thing will be replacing doctors. The first story about silicon is a story about artificial intelligence.

The second story is the story of Fritz. When Deep Blue defeated the world chess champion, humanity was traumatized because chess changed from a game of thought to a game of calculation. However, when Deep Blue defeated the world chess champion it weighed 1.4 tons, had 520 processors, and was capable of

calculating 200 million chess options per second. This was a brute force solution. The more astonishing story is Fritz, which as early as 2009 ran algorithms on a smartphone winning a world class chess champion's match. It's a remarkable story because Fritz calculated fewer than twenty thousand chess modes per second. This is no longer a brute force, but rather a method of processes and algorithms that assess which relevant steps should be considered and taken. It thinks; it activates artificial intelligence. In this manner, Fritz was capable of running on weak hardware, like that found on a smartphone, and demonstrated artificial intelligence already in 2009. This second story uses artificial intelligence and not brute force.

The third story brings us to the DNA level, our own cells. Studies conducted in the Weizmann Institute of Science, Technion, and in Stanford indicate that today we can start developing the first generation of DNA computers, or DNA logic gates. We can fit three million computers into a single drop of water volume and introduce this drop into live cells, performing input-output operations at the cellular level. Upon input a certain protein commences its operation, a certain gene activator sparks, and this can turn into a Turing machine. In parallel to these DNA computers, an Israeli company by the name of Vecoy has developed nano-robots, implementing a virus trap at the nano-level. They have already successfully introduced them into cockroaches and now, nano-traps are traveling through their cells, entrapping, and acting as honeypots for viruses. These are not super computers; in fact, they are extremely weak processing units, however these are computers, or should we say, creatures, robots, or procedures that operate at our cellular level.

The fourth story, which in my opinion was better demonstrated in the previous presentation, is the interface between silicon and carbon on the human brain level. We know how to develop pseudo-micro-switches, a switch that resides on the link between electronics and neurons. We can perform sensing and stimulation from the electronic level all the way to the neuron level.

The fifth story discusses the ability to print organs. 3D printers have already printed bladders dozens of which have been implanted into patients. We already know how to create a bionic ear that has higher hearing functions than that of a human ear because in addition to normal frequencies, the bionic ear can also receive radio transmissions. I wonder when we'll start voluntarily replacing our ears, liver, lungs, and kidneys not only with 3D printed organs but with organs that are also connected to the internet.

The sixth story is the tale of creating and programming life. In 2010, scientists created life: they mixed chemicals using a computer, took the same A, T, C and G and synthesized chemicals in a very long manner. Craig Venter Labs have implemented this into the empty shell of bacteria and actually created bacteria that reproduce, but also bacteria that have a God. An Israeli company, by the name of Geno Compiler, produced a genome compiler: take this and that gene, fetch this activator, place it here, pick up this sequence, activate it like so – and voila!- a new living creature. Maybe one day we'll design bacteria capable of converting waste into oil. We are capable of programming life, currently at the bacterial level, a simple organism. There is no reason that one day this will not amount to a human genome compiler.

The seventh story is about the man-machine interface and the likes of Google Glass. Google Glass changes humanity. In the next 10-20 years we'll see a campaign against Google Glass. The campaign will begin in schools, it will be forbidden to bring Google Glass into an exam. A person wearing Google Glass is constantly connected to a computer. The schools and work places will battle it, but in the end, just as calculators became acceptable, so will Google Glass. The interface of man-machine is changing drastically.

The eighth story is the story of the Star Trek Tricorder. To us it always seemed like science-fiction, a device that can scan and diagnose your illness and recommend treatment. It was science-fiction in the past, but it isn't anymore. Qualcomm Tricorder XPRIZE is a competition in which 250 groups are participating, trying to build a smartphone application capable of diagnosing a medical condition better than a panel of ten experts. Naturally, this app will connect to sensors and in the coming five years we will start walking around with bracelets, electrodes, and so on, measuring our vitals. The samples collected will be used as the smartphone application input. Now remember, this smartphone will run artificial intelligence enabled software, and if it doesn't then it could connect to central computers which will run the artificial intelligence software. This will in fact achieve a complete analysis of our health status and potentially prevent a heart attack minutes before it occurs.

The ninth story is another brain story. The goal of the European brain project is to reconstruct the human brain. They say it will take a few decades.

The tenth story is Facebook and other social media, which are new electronic neural systems that connect us all. Today we're

creating what is called a “multi-human.” Our multi-human has people, computers, technologies, but we’re connected, electronically connected, we are connected through the internet, connected through social media, through this is neural network. Where do these ten stories take us? It’s important that each of us consider this. The last story is of F35 that combines all the stories. It is the last manned fighter aircraft. Today, two thirds of American fighter pilots sit in offices. The next generation of fighter jets won’t have room for pilots in the cockpit. The one after that won’t have an operator on the ground either. We know that this is in development. I find this dangerous, one of the greatest perils out there today because a plane with a human pilot or operator will always lag behind, hence the loser.

Silicon is becoming smarter, the carbon is being hacked. The connectivity is rising and the interfaces are becoming more sophisticated from the level of the molecule, cell, organism, human, and mankind. What is the end game? There are three answers: beginning, middle and end. In the first phase, we are going to outsource our health. We’ll place our health in the hands of the network, as we see developing. We see people with sensors that report back to a central computer, which then makes decisions and in return invokes activators that treat us and prevent heart attacks. I expect that the outsourcing of our health will happen in three stages: stage one is an alert in which people will be warned to pay attention and that they’re in danger, stage two is the patch in which an activator will respond to the alert and fix the problem, and in stage three, people’s bodies will be improved to make them younger, to make the human body better than it is. In the second phase, we will outsource our brain, which is part of the multi-human, part of building a network that connects us all. In the same fashion that each and every one of us consists of hundreds of trillions of cells all connected to a central nervous system and brain, and that some of the decisions are made on the cellular or tissue level, while others are made at the brain function level, similarly the outsourcing of our brain will connect us all to a grid. This grid will be interconnected from the cellular level all the way up to the whole of mankind. In the third and final stage that is completely Sci-fi, but is practically a given, we, humans will transform into information; we’ll become Bag of Bits (BOB). Our physical existence will no longer be dependent on matter, neither silicon nor carbon. We will become pure forms of information, information that may shift from one place to another. And yet, there is another possibility, perhaps we will annihilate

ourselves in the process. Perhaps not all of us will live to see the future, not all of us can access the resources that connect us. Some of us will be left behind, making the topic of social gaps a major point of concern. Is this inevitable? On an optimistic note, the future is still in our hands to an extent, “super intelligence would be to achieve whatever goal it has. Therefore is it extremely important that the goals end up with and the entire motivation system is human friendly.”

Is the Mind the Next Target for Hackers?

Dr. Roey Tzezana | Unit for Technology & Society Foresight at
Tel Aviv University

The world of cyber and connectivity is rapidly overflowing into every niche in our lives. Whereas once the internet was limited to computers alone, today it exists in our shoes, in the smartphones in our pockets, and even, for some, in the glasses that they wear. As the trend of wearable computing keeps moving forward, the exterior of our body keeps getting covered with devices that hackers can break into. This is the near future, but what lies for us even ahead, five or ten years from now?

I would like to posit that by that time, the next target for malicious hackers will be the human brain itself.

Digital and Biological Worlds – Snapping Together

In past centuries the brain was considered an eloquent clock, whose inner workings cannot be looked into until the death of its owner. However, in recent decades we have developed novel ways to gain entry to the brain in non-invasive ways. These ways include, but are not limited to –

- EEG (Electro Encephalo Graph) – a method for sensing the electrical activity of various parts of the brain, and utilizing large amounts of processing power and sophisticated algorithms to differentiate between certain ‘operating modes’ of the brain and to derive meaning out of them.
- fMRI (Functional Magnetic Resonance Imaging) – a method that relies on high-power magnetic fields to measure brain activity by keeping track of cerebral blood flow correlated with neuronal activation.

- NIRS (Near Infra-Red Spectroscopy) – a method that examines the transmission and absorption of near infra-red light in the brain. These parameters respond to hemoglobin concentrations in examined areas, and these correlate to neuronal activation.

Of the above, we will focus particularly on EEG in this paper, since this technology is making first tracks in commercial use by the public. Several EEG devices have been released to the consumers market in the last five years. These include Emotiv's Epoc (~\$300), Interaxon's Muse (~\$135) and Neurosky's MindWave (~\$80). At these prices the devices are available for all, and the software required to analyze their readings is included in the price.

The uses of EEG for the ordinary consumer are generally negligible today. While technology evangelists assert that EEG devices could be used by healthy individuals to direct machines and computers in the household using thought alone, no such use has been found for the technology yet. It is mainly used as either a toy or as a device for providing neurofeedback and keeping track of the brain's functions. Indeed, many are advocating the use of EEG to monitor one's brain in the process of studying and concentrating on tasks. Hence, it is possible that EEG devices would be used specifically by students in the future.

Should the use of EEG grow in society, then it is a certainty that hackers will grow to invade them as well. This sort of intrusion would violate the most sacred sanctum of humanity: the brain and the information that it holds.

Brain hacking has been demonstrated in recent years using EEG devices. In 2012, university researchers have utilized a commercial EEG device to collect confidential information from the 'victims' minds ("On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces, 2012"). The electrodes on the scalp were used to identify points in time when the participants were particularly interested (in a sub-conscious level) in the digits and letters appearing on the screen. The experimenters were thus able to determine which items were related to the participants in response to guiding questions, and find out personal details about the participants, including their ATM pin number's digits.

The described preliminary study reveals how insidious brain hacking can be. Since it can happen on the sub-conscious level, it is theoretically possible for hackers to create a gaming and studying environment in which they can pluck information from their victim's brain without him or her ever becoming aware of the intrusion.

While frightening indeed, the next level of brain hacking calls for even more caution, since it deals with actually changing the inner workings of the brain, rather than simply reading information from it. This is being achieved today, in commercial devices, using a technology called Transcranial Stimulation, in which a magnetic or electric field is being activated in the brain in a non-invasive way.

Transcranial stimulation techniques have shown their mettle in academic testing grounds, and have proven capable of enhancing several cognitive functions, including memory and math skills. Although mainly restricted to lab settings, the first commercial device (called Foc.us) has been released to the public in 2013 for \$250. Foc.us allegedly helps gamers stay at the top of their game, and while hard evidence is sorely lacking for this claim, the device could be considered an early bird of a new type of technology that is beginning to reach the public. If this technology can perform the same kind of cognitive enhancements that it does in the lab, then it seems clear that the public will use it.

The downside of the technology is that it can be used to create negative effects as well, and in fact inhibit certain cognitive functions. Should hackers choose to invade transcranial stimulators and make them influence different areas of the brain than intended, or change the properties of the electromagnetic field, they would in essence have a gateway and a straight road into hacking another person's brain, literally.

Conclusions

The wide public is beginning to use technologies that virtually enable reading and altering the mind. While assimilation of such technologies into society is still years away, regulators and professionals should be aware of the possibilities, and the manufacturers of brain-machine interfaces should include built-in safety measures to protect the privacy – and indeed, the minds – of users.

05

Closing Session: Cyberspace - The Final Frontier?

Cyber Inferno: 7 Circles

Mr. Eugene Kaspersky | Chairman & CEO Kaspersky Lab

Cyber hell speaks many languages, mostly Chinese – all dialects of it, as well as Spanish Portuguese, Russian, Ukrainian and Turkish. It speaks Hebrew as well, not so much, but it does. The result of research on cyber hell is that it is a seven circles inferno. The first circle is full of researchers; it is not too serious. They were innovators and inventors of malicious programs who were writing them in the 1980's. They were the first to develop self-replicating viruses with names such as "brain", which infected floppy disks, to prove the concept of the self-replicating programs. It was easy to kill the virus by simply formatting the floppy disk. The next circle consists of hooligans, vandals who were writing viruses in the 90's. They did it just for fun, to display some funny messages or destroy the data or just doing nothing. That time was also the beginning of the anti-virus industry – to fight with malicious code just antivirus was needed. That was the primitive beginning of the story. The third circle consists of criminals: C2C – criminals to consumers, B2C – businesses to consumers, and B2B as in businesses to businesses. These followed the money and the Internet development in the end of the 90's – beginning of 2000. That was the time when services, like online banking and other, were introduced, which the criminals followed. The Internet services were the victims of these attacks and to fight cyber crime attacks, and Internet suits the task, given the presence of cyber

police forces and the Interpol, which will be operating out of Singapore in 2014. With the help of Interpol, there will likely be more people, not only in the third circle of hell, but also in prisons everywhere around the globe. Kaspersky is supporting Interpol with knowledge and expertise and pledged to their best to control the population of cyber crime.

The cycle number four is made up of hacktivists, who are worse than criminals, because they are not so much after the money, but want to damage reputation or kill businesses. There are many examples for hacktivist activity, such as the Sony Corporation hacks in 2010/2011. But endpoint security solutions that are not solely based on traditional technologies, but on the white lists, where the applications are simply not allowed to be executed, are largely sufficient to fight hacktivists. Circle number five is habituated by espionage, such as Red October or Flame. There are many different groups of people who are behind espionage attacks. It may be independent criminals, who, by chance, got access to classified data they now want to trade to governments or maybe even enterprises, or criminals who are contracted by governments, or maybe even criminals who were arrested and presented with a choice – prison or service. That is why many espionage attacks look like criminal attacks, because they are the same people doing almost the same job – for different clients. To protect customers against this type of threat requires, again, end point solutions, administration tools, but also secure architecture, reduction of unnecessary connections to the Internet, network monitoring capabilities and the like. Education is also needed to explain social engineering to employees of the organizations. Such education is available on the market and afterwards employees are more vigilant, making it more difficult to infect the organization.

The sixth circle are military attacks – nation against nation. Given that there are different points of views in this issue, as well as different ways of definition of cyber weapons, it is still arguable that cyber weapons and cyber military attacks are the worst innovations of this century, because they are malicious, they can travel and infect innocent computers. So cyber weapons are boomerangs. They are also easily mastered so that those who are behind attacks simultaneously act as teachers for the very bad guys who reside in the seventh circle of the cyber inferno – cyber terrorists. In the future we likely will see more and more attacks

that will be defined as cyber terrorists attacks – against nations, regions and global infrastructure.

Unfortunately the world is very vulnerable, it depends on cyber systems – SCADA and PLCs are everywhere. The world cannot sustain itself without telecommunications or technologies. Fortunately and unfortunately the reality is that the world depends on IT and the systems are vulnerable and there will be more terrorists interested in attacks as they continue to learn. I can point out three major cases of cyber terrorism: the attack on Estonia in 2007, the attack on Saudi Aramco in 2012 and the attack on South Korea's banking systems in 2013. The number is likely to become higher, which is why cyber weaponry is the worst innovation in centuries. These bad guys learn from military attacks and espionage attacks and therefore the best way is to protect the cyber space is not technologies, not only through national regulation, but also through strong international cooperation between states to make this world more safe and secure.

Ms. Keren Elazari | Introduction of the Yuval Ne'eman Workshops' Senior Executive Forum work groups

In the context of the dangers of cyber there is a little bit of good news – there are still some good guys and girls. In fact, there are some in the new professions in the cyber age. There are the people with the Red Hats putting on their hacker tool sets to provide Red Team testing in order to promote security. There are teachers and educators concerned with the future of cyber experts, we've got doctors with their heads in the clouds thinking about how cloud computing is to bring about the change and the risks that are involved with it and there are security professionals passionate about sharing their knowledge, information. They are sharing intelligence and helping each other. These are the working groups of the Yuval Ne'eman Workshop. As part of the workshop's activities there are regular events, meet ups, sessions held voluntarily, where professionals, academics, private and public sectors individuals, gather to focus on these areas of expertise.

The most adventurous team, perhaps the team that has the most fun - is the Red Team. These guys contribute with their hacker toolsets and capabilities in order to provide penetration testing and risk assessment in a voluntary capacity, working to promote national cyber defenses with assessments and recommendations. They are providing penetration testing for organizations that are not secure, organizations that are not covered by national defenses. These are security professionals from private and public sectors, some of them are academics, but they all come together. They contribute their time and expertise in order to promote the national cyber resilience of Israel. Some of the examples of their recent activities include looking at how they can hack into

hospitals' medical systems.

Given that education is the future, and kids are the key, there is a need to raise cyber defenders and cyber thinkers. There are fantastic groups and projects in Israel focused on building the next generation of cyber experts. One such example is "the Magshimim" program for talented high school kids who participate in programs after hours in order to learn about cyber technologies and become the forefront of the new cyber warriors.

In cloud computing, the group led by Dr. Guy Tel Tzur focuses on mapping the challenges, the risks and the impacts of cloud computing, which results in recommendations and guidelines on the best ways to secure computing and cloud space. Finally, there is group involved with information sharing. International sharing, though needed and critical, is difficult to bring about. Therefore, the information sharing group got together with a goal of promoting practices of information and knowledge sharing about cyber attacks to promote the overall readiness and security stance of Israeli organization. With assistance from Niv David, a fellow at the Workshop and Mr. Menny Brazilay, a community of security professionals was created. This community has already come together in information sharing meet ups sharing some of their knowledge as well.

There are websites that were targeted in the recent "OpIsrael" attacks. Our group got that information and started sharing and circulating it amongst trusted partners within the network, so that the organizations listed as target could be protected in time. And last but not least, the group is committed to producing a mission statement and guidelines document that is going to really help facilitate information sharing in the private sector in Israel. The group is expected to cooperate on with national organization like the National Cyber Bureau and the national CERT.

In conclusion, there are some fantastic groups coming about and the best thing about it is that people are contributing their own time and their experience to work on a better future, a little bit of optimism in the unsettling context of cyber.

The Applicability of International Law in Cyberspace - From If to How?

Prof. Catherine B. Lotrionte | Director, Institute for Law, Science & Global Security, Georgetown University

The global approach to international cyber security is based on six very important principles. The US government is advised on these, but actually they are appropriate for all nation states, as they deal with the cyber security issues. The first principle is that cyber space is not a unique environment. People forget that it is not some special domain, although it might be manmade. Like in the other domains, states will operate as they always have in this cyber domain, which means that there will be conflict as well as opportunities for negotiating agreement in this environment. The second principle is that cyber space cannot be disarmed. In other words there is no equivalent of a global zero for a cyber attack. States may be able to develop some of the rules of the road that they may agree to, but disarming principles in cyber space is really not an option. In fact, the discussion on arms control and treaties dealing with arms control is the incorrect model to use. In other words, in cyber space it is not about specific weapons that states would outlaw, such as with the chemical and biological and nuclear weapons, while states will continue to act as they do in other places. The third principle is that the world has entered into a period of what some thought of as sustained low-level competition for influence, where the opponent states will have and do have miscalculations and misperceptions, which are a source of risk for all of the nation states. So the importance is, that because there is such a high risk of misperception and miscalculations, a model of strategic ambiguity is very counterproductive to stability in regard to cyber security. Therefore, coming to agreements on specific rules and expectations of how states are to behave in

this environment is very important. The fourth principle is that all nations are better served by embedding the topics and the issues of cyber attack and economic cyber espionage in the already-existing international legal frameworks and international legal agreements that might come to form. That means that there is no need for another word to describe a special new framework in which to work. The fifth principle, and this is related to an immediate goal –is to increase the risk of launching a cyber attack or engaging in malicious cyber activities for both states and non-state opponents, because only by increasing the risks and the penalties and consequences might there be stability in this space. The sixth principle is that there are limits to negotiations in cyber security to decrease risks, and there will always be risk. The goal, though, is to decrease and bound that risk, as part of larger efforts to strengthen international security.

The key to all of this is developing international norms. The international norms are an important part of the framework, but alone they are insufficient, if they are not backed up by action, so states must be prepared to put on the table what their red lines and thresholds are in cyber security and actions between states. Some have argued that declaring red lines is dangerous, because declaring them adversaries will push the limits and may cross those red lines. Therefore states must be prepared to act in response to when that happens. But that always has been the case in international relations, in international security and yet, historically states have benefited from red lines. So developing these norms, coupled with actions by states, is very important. There is a need for such a consensus, because misunderstanding, miscommunication and miscalculation based on misperception exist. An overestimation of the benefits of cyber attacks by the opponents and an underestimation of the costs involved in such actions - so there are dangers with respect to tripping over red lines that states might not be conscious of. This leads to greater instability, escalation and conflict in the cyber domain.

The US has taken a very pragmatic approach and is sought after for what is been considered a middle ground, seeking collaboration, often in bilateral efforts, but through recognition of confidence building measures. These are mainly focused on transparency between states, and also a discussion of possible red lines, of what thresholds will be defined, those actions that the US will accept in cyber space and those actions that are not acceptable. Some of the thresholds and the red lines the US is drawing are worth thinking about: There must be a distinction within the laws,

and in practice of states, between cyber crime and espionage, and that which causes damage and destruction. There is also another line that one can draw in distinction when drafting up thresholds and red line, between damage and destruction of military targets versus damage and destruction of civilian critical infrastructure. And that is one regarding which great effort is being done with respect to how one might be able to draw a distinction, and states might actually be able to incorporate those distinctions into their military operations. The norms of international laws and the threshold do accept a certain level of conflict in cyber space, but what is important is to attempt to increase the costs to the opponent and the consequences to states, if they move beyond the actions, for instance of espionage and crime. This means that the international law needs thresholds of cyber crime and espionage.

Traditionally, individuals do acts of crime and espionage, with respect to the distinction between political espionage and economic espionage in cyber. But for state actions in regard to use of force and conflict in international law, article 2.4 of the UN charter is what is relevant. That is the provision of the charter that prohibits all uses of force against a state's political independence and sovereign integrity. Therefore a state in cyber conflict must analyze what would amount to a use of force against its political independence and sovereign integrity. There is also another provision of the UN charter, which is very relevant in discussing conflict: article 51, which is one of the two exceptions built into the UN charter for actually using force. Aside from article 2.4, which prohibits it, there are two exceptions. One, if the Security Council authorizes the use of force. Two, more importantly, under article 51, if a state suffers an armed attack use of force is justified. Much has been discussed as to what in the cyber domain would amount to an armed attack, because states in deciding whether they are going to use self-defense, they first must decide if they have suffered a use of force, and then they must decide if it reached its threshold of an armed attack. With the publication of the Tallinn manual there is a lot to discuss, debate and to deliberate on this issue.

There are some significant challenges under the international law related to cyber security and to cyber domain and conflict. Here are the largest that still exist: concerns of violations of one's sovereignty are a difficult issue, because traditionally violations of sovereignty in the norm of non-intervention fall below the article 2.4 threshold of the UN charter. So what does one do with respect to

counter measures? If a state has suffered such a wrong, the issue under international law of what are acceptable countermeasures is critically important, still yet a lot of research is needed on this. Third party sovereignty issues of innocent states that basically are passed through and yet who has suffered damages when two other states are engaging in conflicts across their borders. The principles of state responsibility – when should a state be held responsible for cyber negative and adverse cyber activities that are maybe traverse their territory or launched from their territory and do harm to others. What kind of legal responsibility and liability can be imposed upon that state for not preventing it? And then there is the issue of economic espionage, which has been subject of many discussions lately, and the threat thereof. As well as the reality of the IP theft that states like the US has suffered. These have become key issues of international security.

The difficulties with cyber in comparison to other issues in international law, although it is not to say that international law could ever be irrelevant, because it is, it is more about how nations go about applying it. The challenges are certainly more complex. Enemies, adversaries and opponents are more invisible than traditionally. The damage can be delayed for quite a long time, for example with a logic bomb waiting to be triggered inside a system. Dual use technology as such in other areas also challenges those that are looking to develop policy and rules about cyber space. The actions of non state actors who have been become very powerful just as in terrorism and the time frame for the actual cyber incidents being short, where a state might not have time to respond in self defense. These are just a few of the challenges that policymakers and lawyers face when they try to analyze and apply the international law.

Luckily, the debate has moved on in the last couple of years. Originally when discussing the laws and the rules which apply in cyber space, there were pushbacks - the applicability itself was questioned. Most of the debate has gone past that and now there is a general international agreement that some of the international laws indeed apply. Now the more difficult work is being done, it needs to be done. It is still in a very basic phase of just how those rules apply in cyber space, at least there is no longer this doubt of whether they are applicable. Now the community just must work together – technologists, academics, practitioners and business people – to find out how to apply these rules, which have existed for hundreds of years, in the new environment. Whereas states will continue to operate in this environment as

they have operated in other domains and therefore nations must be prepared to experience, not the 'cyber Pearl Harbor', but continuous controversy and conflict in cyber space. There also will be potential, and hopefully the results of agreement and cooperation on some of the norms will actually create the bounds for acceptable behavior.

Terror Pornography, Gateway Websites, Drive-Thru Radicalization and Jihadi Cyber Weapons

Dr. James Van de Velde | Lecturer, Center for Advanced Governmental Studies, Johns Hopkins University; Associate, Booz Allen Hamilton

Paraphrasing the well-known saying, it can be argued that “You may not be interested in cyber jihad but cyber jihad is interested in you”. The cyber domain is the fifth domain of warfare and what’s unique about this domain is that humans created it. If Delta, American Airlines and El Al all owned airspace and had allowed al-Qaida to fly through it, they would probably have a say in that activity.

It is well-known that al-Qaida has a series of official websites where they propagandize the world, they have a number of mirrored sites and they have hundreds to thousands of wannabe sites. It is thought this Internet that al-Qaida maintains a global following and a certain command and control. At the moment al-Qaida uses the web for inspiration, recruitment, planning, information sharing, organization web posting. At the same time the West more or less tolerates this, a more aggressive conservative US government might tolerate it at least, but in general the West allows this to happen.

The next level however might be less tolerable to the West. Should jihadists move to CNE, probe networks and engage web defacement, the attitude in the West would likely become less permissive. These acts will probably not be acceptable to the West and following that the third level of cyber activity would be weapons that actually attack al-Qaida systems, bots or implants. These activities would be highly damaging and very upsetting to the West. They would also likely be met with some sort of response. In a sense, the Internet at the moment is a gateway drug for al-Qaida, a sort of marijuana, where it has already

established a certain level of presence and likely is to move to the next level and then to the worst level. Jihadists internationalize their fight through the cyber world, and the center of that cyber world is flat. Individuals worldwide who otherwise might not have access to al-Qaida's message can see it anywhere. An al-Qaida senior member in the Middle East could radicalize someone in Mexico, Texas or Paris. Given the very heavy kinetic stress that the West has placed on al-Qaida, it is arguable that the al-Qaida senior leadership was nothing more than a pornography studio, where they produce this junk and post it on the West. But the role as a planner, an operator, a deviser of plots and implementer has really faded away in a sense that they do inspire a projected image worldwide. In a fact, the very senior leaders of al-Qaida are, in a sense, pornography pimps, because they no longer plan anything at all. Instead they just try to ask the rest of the world to share their ideology and act accordingly.

For al-Qaida terrorism is a form of performance art. It's the image that they are trying to seal now, in addition to the activity, and that image is delivered through the web. Some have called this phenomenon cyber insurgency. How can a cyber insurgency be defeated? First, the performance art should not be shown. Largely the West, or at least the median in the United States, seems to show terrorism less and less. It may be due to a function of the president's agenda, it may be due to a strategic decision made by accident and it is a good thing. Showing it of course advances the enemy's information operations, it is one element of warfare, perhaps al-Qaida senior leadership's only relevant element of warfare.

The second way to defeat performance art is by showing that it is wrong, to counter the message, the brand. In a sense al-Qaida has been denied safe havens around the world, resulting in them establishing virtual safe havens. But this means that the Internet is a sort of al-Qaida and exists for jihadist wannabes around the world. Anyone, anywhere can be radicalized by merely going to the web, getting his fill of the propaganda and the message and the narrative of al-Qaida and, if necessary, learn where to go to meet individuals in person around the world and then return home. In fact, a study in the journal of social behavior argues that the Internet has fostered a sense of self in the community and therefore the Internet is becoming the mentor for the local jihadist. Terrorism has been extensively studied in the United States, trying to understand what makes an individual radically violent. It is known that not every radical becomes violent, but

one commonality is that a small sense of community is needed. It can be a study group and from that study group an individual is afforded the support mechanism. He or she is not required to actually committ violence.

The Internet is becoming that mentor, that friend. Social networks are only going to make things much worse and al-Qaida is already in social networks – Facebook, Bing, and is also building its own social networking forums. These are tools of the jihadists today and are likely to be only furthered and developed in the future. File sharing, talking through web 2.0 technologies, these will only make efforts at counterterrorism more complicated. And worse, since the Internet presence already exists and they are already infected with this tool, al-Qaida may move from simple web 1.0 technologies, 2.0 social networking to more destructive code – jihadist cyber weapons. But unlike conventional weapons, delivery of such programs may be much easier, have little to no lead time required and may not require any particularly skill. To date, al-Qaida has not showed extensive interest in cyber weapons, probably for two reasons: one, they were not spectacular enough – al-Qaida was determined to follow 9/11 with an equally spectacular attack. Two, technically it has been a beyond their reach, but it is perhaps less so these days. Foreign governments are big actors of cyber space and developers of cyber weapons. Foreign governments like Iran have significant cyber efforts and weapons. But unlike WMDs, where there is a lead-time, where it is possible to watch a weapon's development program, for example in Iran, cyber weapons do not necessarily have such a lead-time. A cyber weapon can be given to a member of al-Qaida developed elsewhere. Access can be given by a foreign government rather than developed. Traditionally, WMD were tracked – not only while the weapon was developed, but also the delivery mechanism was tracked. With cyber weapons there is no such luxury. Space, time and geography are no longer defenders for the West. Overnight al-Qaida could become a cyber weapon power, if it was given a weapon. There is some reason to suspect that this is coming. In the latest edition of "Inspirer" – the propaganda mechanism al-Qaida in the Arabian Peninsula, the authors called for individual jihadists to merely spread oil slicks on street corners and to nail nails into boards to create flat tires in cars. It is pathetic – al-Qaida now calling to kill individual soccer moms and old men is a far cry from their 9/11. So if they have given up their interest in a spectacular follow up of 9/11, what would prevent them from any sort of disruption of using cyber weapons?

Today al-Qaida seems to be calling for any attack anywhere, even for individuals to pick up a weapon. A hacker group like Anonymous, a very capable hacktivist, could provide such weapons overnight, and it may not even be done by the group as some sort of sanctioned act. Maybe, a single individual is tricked to give a weapon or is individually sympathetic and it is not inconceivable that a state like Iran would give al-Qaida a weapon just to make trouble for the West to create an asymmetrical war for the United States.

The forensics in such an activity would further complicate – there might be an Iranian weapon or even a Russian or Chinese acquired by Iran given to al-Qaida delivered through individuals and networks around the world from addresses in Southeast Asia, Canada, Texas. Regardless of who took responsibility for the weapon, it would be a nightmare for the West to understand who created the weapon or who to retaliate against. This means in general that al-Qaida does not necessarily need to develop anything, although there the trend towards one's own expertise is visible. This suggests they would take such aid if offered, but if not, they are going to try to train themselves in these weapons. The legal advisor for the US Department of State has claimed that international law applies to cyber space; cyber activity can constitute the use of force. A state may respond to a computer network attack by exercising its right to national self-defense. The law of armed conflict applies to cyber tools and hostilities. In other words cyber warfare is warfare. Trotsky was right; cyber jihad is of concern to everyone.

Appendix: Yuval Ne`eman Workshop for Science, Technology and Security - Researchers' Articles

Critical Infrastructure Protection (CIP) against Cyber Threats: the International Cooperation Imperative Lior Tabansky

What Makes an Infrastructure Critical?

A functioning modern society depends on a complex tapestry of infrastructures: energy, communications, transportation, food, and many others. An infrastructure is a system that combines various facilities and enables certain activities, for example, a pipeline that conducts water from wells to homes and fields, paved roads, bridges and intersections that allow movement of people and goods, flight, communications, fuel, and health services. One of the properties of an infrastructure is the dependence of various spheres of activity on it. In the past, the dependence stemmed from physical or geographical relationships only. With the development of cyberspace, which includes data communication systems and computerized command and control, there are additional relationships, which in turn create new vulnerability.

In the information age, traditional infrastructures become information infrastructures because they incorporate computerized devices. In addition, new critical infrastructures have been created that are purely information infrastructures: computerized databases that contain important data, such as records of capital in the banking system, scientific and technical intellectual property, and the programmed logic that manages production processes and various business processes.

The Novelty of the Threat

Infrastructure is defined as critical when it is believed that disrupting its function would lead to a significant socio-economic crisis with the potential to undermine the stability of a society and thereby cause strategic consequences. Three factors are considered to estimate the criticality: the symbolic importance of the infrastructure, the immediate dependence on infrastructure, and complex interdependencies where failure of one component may cause a wide range of outcomes.

Recent years have brought increased concern over the potential vulnerability of developed modern society's infrastructure, yet the fact that this discussion is taking place now is surprising. Critical infrastructures importance has always been obvious. Conflicts

are not new to the world, and in war it is only trivial to attempt to harm the adversary's critical infrastructures. In 1917, during the Bolshevik Revolution, Lenin and Trotsky ordered their activists to take over the post office, telegraph, bridges, and train stations. In prolonged wars, such as the Second World War "strategic bombing campaign" huge efforts to hit critical infrastructures in order to interfere with the enemy's fighting ability and spirit were made. A country's critical infrastructures, whatever they are, are elemental targets during a conflict, and therefore organizations and states have labored throughout history over defense systems for their infrastructures: camouflage, guarding, fortification, defensive forces, deterrence, and so on. Why, then, is there a growing concern of damage to critical infrastructures, particularly in the strongest developed countries enjoying total military superiority over their respective enemies? The US or Europe have not experienced wars on their territories in recent decades. Israel is the only developed democracy that is under ongoing military threats (Iraqi SCUD missile attacks in 1991, Palestinian suicide bombers in 2000-2005, and current short range rockets attacks from Gaza, Lebanon and Sinai).

Identifying the enemy is critical for response and deterrence. In all forms of traditional warfare, the identity of the enemy is disclosed following the attack because in order for the attack to be carried out, the weapons must physically reach the target.

Thus what prevented harm to critical infrastructures in the past was the defensive force placed in the path of the enemy, and even more so, deterrence promised to exact a heavy toll. This familiar state of affairs came to an end with the development of cyberspace. For the first time in history, it is possible to attack strategic targets (such as critical infrastructures) without physically reaching the location, without confronting defensive forces, and without exposure of action and identity. The major challenges stemming from the characteristics of cyberspace as it exists today are:

- vulnerabilities of computerized systems and the widespread use of off-the-shelf commercial technologies
- difficulty distinguishing a glitch from an attack
- establishing a causal link between an event and a result
- tracing the source of the attack
- identifying the attacker, even if the geographical location is known

Layers of Critical Infrastructure Protection

Confronting the threat includes prevention, deterrence, identification and discovery of the attack, response, crisis management, damage control, and a return to full capability. Proposed here is a division of methods for confronting the threat to critical communications infrastructures to technological, national-strategic levels and supra-national. All the levels are required to confront the threat, but given the different focus, it is worthwhile distinguishing between these levels of protection to identify the essence of the challenges of protecting critical infrastructures particular to cyber security.

The problem is perceived as a technical one, and therefore, the proposed solution is an engineering solution. The technical and operational layers for confronting the cyber threat focus on identifying vulnerabilities in an organization's computerized systems and seek engineering solutions to reduce the vulnerability.

The National Strategic Layer

The national strategic layer examines CIP in the national security framework, beyond the boundaries of an organization or a business process but as part of the protection of society as a whole. CIP actually becomes protection of an information-based society. Information security, which is at the center of the technical level, is a necessary but insufficient part of the strategic vision.

In a national perspective, a comprehensive national policy on protecting critical infrastructures is needed, which in addition to the engineering foundations must take into account the complex social, political, economic, and organizational aspects. An organizational entity capable of taking into account the complex of relationships between critical infrastructures and a functional society and the state is also required. The national level of protection requires cross-organizational activities, backed by effective authority. This is a complex challenge for public policy, considering the structural limitations of public service on the one hand and a required level of strategic focus of those in the private sector, on the other.

The Supra-National Layer

The trans-national character of telecommunications network and the Internet is widely acknowledged. Any discussion or official document on cyber security stresses the need for international cooperation, norms and rules of conduct. However, given the structure of international system as described by the Realist

theory of international relations, such cooperation is extremely unlikely. Is the future of cyber security and CIP doomed to isolated, national endeavors?

International organizations hold a promise to an intriguing solution for the CIP problem. Without delving into the legal and formal definitions, alliances such as NATO or ASEAN are voluntary cooperation between like-minded states. The motivation for such an extraordinary cooperation in view of the Realist theory of international relations is the presence of a common security threat. Civilian CIP could provide further common ground for a continuous cooperation. From a non-member state perspective, it appears that the sort of joint endeavor enabled by NATO will provide the member-states an exceptionally valuable added layer of protection.

Issues for Policymakers

The information revolution continues to affect a range of social, cultural, and economic issues in complex ways. Cyber security, Critical Infrastructure Protection in particular, is already on the policy agenda. In spite of the great similarity in the threat there are differences in the framework of the discussion and the types of solutions proposed in different countries. The differences must stem from the role social institutions play in the discussion and in determining the response. What follows are the main issues concerning cyber threats that call for a public debate.

Any discussion on protection and defense measures must begin with prioritization. An assessment of how critical an infrastructure is on a national level must address the full matrix of social values, goals, and interests. Therefore, the relative importance of infrastructure and the amount of public investment needed to protect it are not derived from an engineering formula, and require a wide ranging and informed public discussion. The central challenge in designing a policy to protect critical infrastructures from cyber threats is not technical or operational, rather a challenge of a comprehensive national-strategic vision. Critical infrastructure protection is not the exclusive preserve of systems engineers and computer experts. The optimal CIP can only be created through a broad public discussion in the framework of a democratic political system. Given the constraints of the political system, such a discussion will presumably be lengthy and at times frustrating. Nevertheless, only through a joint political process will it be possible to design an optimal response to the threat for the long term.

The transnational character of cyberspace is widely acknowledged. On the international level, cooperation is only likely to occur via alliances of like-minded states. Therefore, states that already enjoy membership in an alliance such as NATO or ASEAN already enjoy a structural advantage in cyber defense. Since 2002, through the oversight and guidance of a dedicated organization, the State of Israel has been protecting infrastructures it deems critical. Despite the relevant success of the Israeli approach, the lack of participation in formal international alliances may impede the CIP effort. Indeed, the major challenge in protecting critical infrastructures from cyber threats is not technical, but strategic and political.

Conclusion

Above the national level, international cooperation is beneficial for CIP; alas cooperation is highly unlikely in the anarchic international system. Thus, participation in an alliance like NATO or ASEAN holds an intriguing opportunity to enhance the strategic posture of its members in the information age. If this potential will be fulfilled, the international level of protection will enable an additional unique shield to the member states. For Israel, the situation presents an opportunity: with the newly reinvigorated national cyber-policy, the Israeli leadership should leverage the national technical and operational prowess to promote international cooperation for CIP with like-minded countries, as both technical and national policy layers might be no longer sufficient for Critical Infrastructure Protection.

A Multi-Faceted Strategy for Cyber Standardization

Deborah Housen-Couriel, Adv. and Admit Ivgi, Adv.

• Introduction: The Role of Standardization and its Importance for Cybersecurity

Standardization is of core relevance to preserving the confidentiality, availability and integrity of digitized information stored in computer systems and transmitted among them over communications infrastructures, including wired and cabled systems, wireless relay, satellites and undersea cables. Moreover, standards play a key role, both actual and potential, in defending against the present dramatic rise in the number and intensity of cyber attacks being carried out against targets embodying the strategic interests, concerns and agendas of state and non-state actors. Because of their particular characteristics and attributes, standards can serve as an effective tool of policy implementation in the long-term planning of states and international organizations to enhance cybersecurity at several levels. This article proposes that the optimal application of cybersecurity standards requires a multi-faceted strategy on the part of states and organizations, to include approaches such as strategic adaptation to technological developments, incident response, and sector-specific technical development.

Standardization organizations such as the IEEE, IEC, ISO, IETF, ITU and others have traditionally focused their standardization strategy for network security on the familiar triad of critical cybersecurity concerns: confidentiality, availability and integrity (sometimes referred to as “CIA”), although this concept is now evolving to include a broader range of elements due to developments such as ubiquitous cloud computing. Moreover, challenges posed to network operators such as abuse of system capabilities, malware, insider threats and other types of attack now require a strategic and multi-faceted approach to cybersecurity standardization. For example, The “Saudi Hacker” cyber-attack against thousands of Israeli credit card payment holders’ databases, in January 2012, might have been prevented or mitigated if the PCI-DSS standardization (“Payment Card Industry Data Security Standard”, discussed below) had been mandatory for Israeli credit card companies. Ongoing work in the standardization organizations referred to above to develop standardization tools such as the

ISO/IEC 27000 series and the Internet Security Forum's Standard of Good Practice, will boost intergovernmental efforts to meet the twin challenges of identification and attribution in cyber-attacks, if sufficiently adopted and enforced. To achieve this aim, a multi-faceted strategy for cybersecurity standard adoption and enforcement as a core element of cybersecurity policy is needed at the national, regional and global levels.

• **Cybersecurity Standards**

Cybersecurity standards are not a new development, although the constantly-evolving challenges of cybersecurity are influencing current versions. They have evolved in diverse contexts in recent years, including national laws, some of them initiated in anticipation of future cybersecurity challenges, some on an incident-response basis and some in accordance with sector-specific technical development. An early example of incident response-based standards that focus on the integrity of financial databases as an integral part of corporate governance, was prompted by the Sarbanes-Oxley Act of 2002 ("SOX"), specifically in its Sections 302, 404 and 802. SOX is a United States federal law, adopted in its essence by several other countries, that set new or enhanced standards for financial database integrity incumbent upon all public company boards, management and public accounting firms regarding the integrity of corporate financial databases and their protection. The bill was enacted as a reaction to a number of major corporate and accounting scandals in the US, such as the 2001 Enron scandal, that occurred when companies' databases and information systems were fraudulently altered. As a result of SOX, penalties for fraudulent financial activity, including database corruption, became significantly more severe; and the oversight role of boards of directors and of auditors responsible for reviewing the integrity of corporate financial records was dramatically increased. The widespread digitization of such records rapidly prompted the development of professional standards to protect the integrity of such data, specifically ISO/IEC 38500, entitled "Corporate Governance of Information and Communication Technology", initially published in 2007.

Another example of standardization processes in response to fraudulent activity is the establishment in 2006 of the Payment Card Industry Security Standards Council by the five leading payment card financial institutes: American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, as a response to the fact that, in 2005 alone, more

than 234 million records with sensitive information had been breached. The standardization initiative was intended to increase controls around cardholder data and reduce credit card fraud. Accordingly, the Council established the PCI-DSS standard for entities that transmit, store, and process credit data.

Finally, the ISO (International Standardization Organization) family of information security and technology standards, which plays a leading role in cybersecurity and other types of standardization, provides a strong example of standards which aim to anticipate future challenges to network security. They provide a risk-based management system that specifies the overarching structural requirements for information management frameworks. As such, they are flexible and allow for the characteristics of the specific organisation at the level of implementation. The most relevant of ISO's standards in this context is the 27001 series, encompassing nearly 30 different standards for the management of information security under the Information Security Management System rubric (ISMS). One of them, ITU-T X.1054 (entitled "Governance of information security") has been jointly developed with the ITU and was updated in 2013. In addition to international standardization efforts, several countries have begun to develop standards at the national and regional levels. We shall now see how this trend reflects in the United States' and the EU's cyber-security standards, specifically regarding critical infrastructures.

(2.1) The US Framework for Improving Critical Infrastructure Cyber Security

One recent example of standardization governing the cybersecurity of critical infrastructure in the United States is the extensive reference to standards in the 2014 National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cyber Security". The Framework developed in the wake of President Obama's Executive Order 13636 "Improving Critical Infrastructures Cybersecurity" of February 2013. The Executive Order established that "[i]t is the policy of the US to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." Section 2 of the Order defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the US that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health

or safety, or any combination of those matters.” This broad and innovative definition is in fact relevant not only to “classic” infrastructure such as electricity, water, transportation, and gas, but also to the newer and mostly private-sector infrastructures such as those relevant to e – commerce (Ebay, Amazon), online trading (Forex), cellular telephony and social media networks (Facebook, Twitter, Google). In support of the implementation process of Order 13636, in February 12, 2014, NIST published the Framework, which focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework was developed together with private sector entities, and consists of three parts: (1) the “Core” – a set of cybersecurity activities, outcomes, and informative references that are common to most CI sectors; (2) the “Profile”, which guides organizations in aligning their cybersecurity activities with business requirements, risk tolerances, and resources; (3) and the “Implementation Tiers”. Appendix A, which describes the Core, specifies in detail the relevant standards for each function in the NIST Framework, including those formulated by COBIT, ISO, IEC, NIST, CCS CSC, and ISA. Standards have thus become an integral part of the US’ current cybersecurity strategy, promoted at the federal level as a key tool for implementing overarching, national goals.

(2.2) Standards and the Cybersecurity Strategy of the European Union (EU)

The EU relates to digital technologies and the internet as part of the backbone of European society and economy, and as key enablers of regional prosperity and individual freedoms. In addition, the EU has committed to a high level of network and information security across member countries, as essential to ensuring consumer confidence and helping to preserve the functioning of the European internal market by boosting growth and jobs. Standards are an important part of this process: Pillar II of the 2010 Digital Agenda for Europe is entitled “Interoperability and Standards”, and specifies the regional strategy for cybersecurity standards development to support overall EU cybersecurity policies. It is related to several other EC initiatives, including the March 30, 2009 Communication on Critical Information Infrastructure Protection (CIIP) and the 2013 Proposed Directive on Network and Information Security and Cybersecurity Strategy. These three initiatives will be briefly reviewed, as examples of the substantive basis for European cybersecurity standards. The 2009 Communication focuses on the protection of regional infrastructure

from cyber disruptions by enhancing security and resilience. It launched an action plan, involving both Member States and the private sector and based on five elements: (i) preparedness and prevention, (ii) detection and response, (iii) mitigation and recovery, (iv) international cooperation and (v) criteria for EC critical infrastructure in the field of ICT. Based on the CIIP and in further broadening the regulatory structure for cybersecurity, on February 2013 the Commission published a proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. In order to ensure convergent implementation by Member States, the proposal requires that both countries and the Commission encourage the use of relevant standards, and that EC draw up a list of these. Together with the Proposal, the Commission published in February 2013 a new Communication on a Cybersecurity Strategy of the EU – An Open, Safe and Secure Cyberspace. And in the same vein as the Proposal, the Strategy endorses the adoption of existing standards and to developing of security standards in particular in critical economic sectors. In order to optimize implementation of these and other EC policies, on April 2, 2014 the European group Standardization Organizations (ESOs) presented their latest proposals for maximizing the positive contribution that standards can make to enhancing cybersecurity and personal data protection.

• Present Trends and Conclusion

The use of standards to promote various aspects of cybersecurity policies, especially those relating to the protection of critical infrastructures, supports the enforcement of domestic and regional regulatory norms. The analysis above looks briefly at the United States and the European Union as actors that have included standardization as important underpinnings of their policies. Interestingly, both actors have connected standardization initiatives to policy initiatives, while maintaining a separation and in large part refraining from requiring organizations to implement specific standards. As cybersecurity policies grow in sophistication, and regulators such as the US government and the EC require a higher level of corporate responsibility from private-sector organizations, we anticipate that standards will be more readily used as a core tool of cybersecurity policy. Their wider adoption will require a multi-faceted strategy for cybersecurity standardization, as outlined above.

Participants' Biographies

(In Alphabetical Order)

Mr. Michael Arov | Head of Information Security, R&D Section, RAFAEL, Advanced Defence Systems

Head of Information Security, R&D Section, RAFAEL, Advanced Defense Systems. Mr. Arov engaged in research and challenges of the cyber world and he has an extensive experience in management and initiating of R&D on advanced cyber issues. Mr. Arov is a security architect for networks, organizations, weapons systems and more.

Mr. Curt Aubley | VP/CTO Cyber Security & NexGen Innovation, Lockheed Martin

Mr. Aubley is responsible for leading the creation of next generation cyber security, cloud computing, mission focused IT Innovations, service management, mobile, and integrated solutions, across LM IS&GS lines of business for their world wide government customers. Mr. Aubley is the recipient of three prestigious Lockheed Martin Nova Awards, LM IS&GS Eagle, and three President Awards. He has published articles and papers for: Lockheed Martin, Department of Defense, Sunworld Magazine, Windows NT Magazine, InfoWorld, Windows Magazine, and LMIT's Precision customer publication. He has also authored two books published by Prentice Hall: Tuning and Sizing NT Server & Tuning and Sizing Windows 2000 for Maximum Performance which are both in their second printings.

Ms. Carmela Avner | The Government CIO

Ms. Carmela Avner - Government Chief Information Officer. Ms. Avner is the Government CIO since 3/2012, the first to hold this position. She previously served as director of Israel's e-Government program. Ms. Avner holds an EMBA specializing in International Business Management from the Kellogg-Recanati International Executive MBA Program of Tel Aviv University, and a BA in Industrial Engineering from Tel Aviv University. Prior to joining the public sector Ms. Avner held a number of high profile positions within the Israeli Hi-Tech industry, acting as a VP at Ness Technologies, Global Operation VP and CIO at NICE and additional senior management posts at EDS (known as HP today) and Teva pharmaceutical.

Mr. Ehud Barak | Israel's Minister of Defense

Lt. General (Res.), former Chief of General Staff of the IDF, member of the Knesset, a Minister and the Prime Minister of Israel between the years 1999-2001. Mr. Barak had received a B.Sc. degree in

physics and mathematics from Hebrew University of Jerusalem (1968) and an M.S. degree in economic engineering systems from Stanford University in California (1978). Mr. Barak was appointed as the Minister of Defense in the Israeli government from 2009 to 2013.

Mr. Menny Barzilay | Head of IT Audit, Bank Hapoalim

Mr. Barzilay is the Head of the IT Audit department in Bank Hapoalim group. He is in charge of all IT Audit activities in the bank, in its branches and its subsidiaries around the world. As part of this position he is working directly with the board of directors and senior management, providing consultant services with regards to Information Technology and Cyber Security for the entire group. Prior to this position, Mr. Barzilay was a CISO in the Israeli intelligence forces. Mr. Barzilay is a member in the senior forum of Yuval Ne'eman Workshop for Science Technology and Security.

Prof. Maj. Gen. (Res.) Isaac Ben Israel | Head of the Yuval Ne'eman Workshop for Science, Technology and Security, Tel-Aviv University

Major Gen. (Res.) Professor Isaac Ben-Israel serves as Head of the Interdisciplinary Cyber Research Center (ICRC). Additionally, he serves as Chairman of the Yuval Ne'eman Workshop for Science, Technology and Security, Chairman of the Israeli Space Agency and Chairman of the National Council for Research and Development in the Ministry of Science. In January 1998 he was promoted to Major General and appointed as Director of Defence R&D Directorate in IMOD. During his service he received twice the Israeli Defence Award. After retirement from the IDF, Prof. Ben Israel joined the University of Tel-Aviv as a professor. Prof. Ben-Israel was also a member of the 17th Knesset (Israeli Parliament) between June 2007 and February 2009.

Mr. Martin Borrett | Director of the IBM Institute for Advanced Security Europe

Mr. Borrett is the Director of the IBM Institute of Advanced Security in Europe. He leads the Institute and advises at the most senior level in clients on policy, business, technical and architectural issues associated with security. Mr. Borrett leads IBM's Security Blueprint work and is co-author of the IBM Redbooks "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security" and "Understanding SOA Security". He

is Chairman of the European IBM Security User Group community and Chairman of the IBM UKI Technical Consulting Group. He is a member of the board of EOS, the European Organization for Security. He is a Fellow of the British Computer Society, and a Chartered Engineer (CEng) and member of the IET.

**Dr. Moran Cerf | Neuroscientist, UCLA and NYU
and ex-security expert**

Dr. Cerf completed his Ph.D. at Caltech, working with Drs. Christof Koch and Itzhak Fried. He is currently a postdoctoral fellow at UCLA with Dr. Fried and at Caltech with Prof. Christof Koch. Prior, Dr. Cerf worked for several years in the Israeli high-tech industry as a hacker. His set of studies include examining the conscious control of single neurons in humans, the ability to affect altered states of consciousness as dreams or sleep, and - in collaboration with Ralph Adolphs at Caltech - the ability of humans to regulate high-level emotions.

**Mr. Ilias Chantzios | Senior Director, Symantec Government
Affairs—EMEA and APJ**

Mr. Chantzios is Senior Director of Symantec's Government Affairs programs for Europe, Middle East & Africa as well as the Asia Pacific and Japan regions. Mr. Chantzios represents Symantec before government bodies, national authorities and international organizations advising on public policy issues with particular regard to IT security and data risk management and availability. Prior to joining Symantec in 2004, Mr. Chantzios worked as legal and policy officer in the Directorate General Information Society of the European Commission focusing on information security policy. Mr. Chantzios holds a law degree from the University of Thessaloniki and a Masters degree in Computers and Communication Law from the University of London and is a member of the Athens Bar.

Mr. Avi Chesla | CTO, Radware

Mr. Chesla is Chief Technology Officer at Radware, where he is responsible for leading the Company's strategic technology roadmap and vision. Prior to the CTO position, he led Radware's security division as VP of Security. Mr. Chesla has authored a number of articles for major publications in the areas of advanced network behavioral analysis and information security and has earned numerous patents in these areas. His views on industry trends and best practices have been featured in articles, white

papers, and on the conference speaking circuit. He holds a B.S. in physics and mathematics from Tel Aviv University.

Mr. Richard A. Clarke | President, Good Harbor Security Risk Management, Former Special Advisor for Cyber Security to the President of the USA

Mr. Clarke was Special Advisor for Cyber Security to the President of the United States. Prior to that, he was the White House's National Coordinator for Security, Counter-terrorism, and Critical Infrastructure. He is the President of Good Harbor Consulting, a cyber security risk management consultancy in Washington, DC. Mr. Clarke served in national security positions in seven administrations, in the Pentagon, the State Department, the Intelligence Community, and an unprecedented ten consecutive years in the White House serving three Presidents.

BG (Ret.) Yair Cohen | Head of Cyber Security, Elbit Systems

BG. (Ret.) Yair Cohen, head of Cyber Security, Elbit Systems. Mr. Cohen served as Vice President of Elron Electronic Industries Ltd. and in Clal Energy. He also served as director of several companies in Elron Group. Mr. Cohen served thirty-one years in the IDF, and in his latest rule he was the commander of the central collection unit of the Intelligence Corps (8200).

Mr. Art Coviello | Executive Vice President, EMC, Executive Chairman, RSA

Mr. Coviello is responsible for RSA's strategy as it delivers EMC's global vision of information-centric security. With more than 30 years of strategic, operating, and financial-management experience in high-technology companies, Mr. Coviello's expertise and influence have made him a recognized leader in the industry. He plays a key role in several national cyber-security initiatives and has spoken at numerous conferences and forums around the world.

Mr. Paul de Souza | Founder & President, Cyber Security Forum Initiative (CSFI)

Mr. de Souza is the Founder/President of CSFI (Cyber Security Forum Initiative) and its divisions CSFI-CWD (Cyber Warfare Division) and CSFI-LPD (Law and Policy Division). Former Federal Director of Training and Education for Norman Data Defense Systems, he also teaches PSSS 6247 Cyber Defense Strategies at George Washington University. He has consulted for several

governments, military organizations and private institutions on best network security practices and also presented in Estonia, the country of Georgia, Australia, Sweden, Czech Republic, Belgium, and all across the United States.

Mr. Andrey Dulkan, Director of Cyber Innovation, Cyber-Ark
With over 12 years of experience in information security research and development, Mr. Dulkan heads the Cyber-Ark Research Labs. He manages the Cyber-Ark innovation and research processes, focusing on targeted attacks mitigation, critical infrastructure security and various aspects of organizational information systems protection. Mr. Dulkan is an active participant in the Cloud Security Alliance Security-as-a-Service workgroup, as well as various other cyber security forums and initiatives.

Ms. Keren Elazari | Introduction of the Yuval Ne'eman Workshops' Senior Executive Forum work groups

Ms. Elazari is an international public speaker and a key member of the Israeli Cyber Security industry. Since 2000, Ms. Elazari has worked with leading Israeli security firms, government organizations, Global Big 4 and Fortune 500 companies. Ms. Elazari holds the CISSP diploma for security professionals, a BA degree in History and Philosophy of Science and is currently a research associate with the prestigious Security Studies program at Tel Aviv University. In the recent years, Ms. Elazari has organized, hosted and participated at many international security and media events such as RSA conference, NATO's International conference on Cyber Conflict, WIRED magazine's UK event, DLD events in Germany, TEDxTransMedia and more.

Prof. Yuval Elovici | Director, Deutsche Telekom Laboratories at BGU

Prof. Elovici is the director of the Telekom Innovation Laboratories at BGU and an Associate Professor at the Department of Information System Eng. at BGU. He holds B.Sc and M.Sc degrees in Computer and Electrical Engineering from the Ben-Gurion University, and Ph.D in Information Systems from Tel-Aviv University. He serves as the head of the Software Engineering program at BGU for two and a half years. Prof. Elovici also professionally consults in the area of the cyber security. In the last seven years he has lead the cooperation between BGU and Deutsche Telekom.

Mr. Mark Gazit | General Manager,**NICE Intelligence Solutions, NICE Systems**

Mr. Gazit is a prominent executive with 20 years of experience as a senior manager and director of several Israeli and international high-tech companies. Mr. Gazit served as a General Manager of Nice Cyber & Intelligence Solutions, an autonomous division of Nice Systems Ltd., which provides software and hardware solutions to the Government Agencies worldwide in the areas of Information Intelligence, Cyber and Safe Cities. Prior to Nice as a Group President and CEO, Mr. Gazit took SkyVision from a start-up stage to a \$100M company serving over 50 countries worldwide and operation centers on three continents.

Mr. Misha Glenny | Writer and broadcaster, Author of “DarkMarket: Cyberthieves, Cybercops and You”

Mr. Glenny is an award-winning writer and broadcaster whose latest book DarkMarket: Cyberthieves, Cybercops and You on cybercrime and its consequences is now being published in over twenty editions around the world. A former BBC Central Europe Correspondent who covered the revolutions in Eastern Europe and the wars in the former Yugoslavia, Mr. Glenny has written for most major publications in Europe, the United States and Japan. In January 2012, Mr. Glenny took up an appointment as Visiting Professor at Columbia University's Harriman Institute. In October 2011, he was named the UK's Information Security Journalist of the Year for a series of articles detailing the relationship between IT security and politics.

Mr. Avi Hasson | Israel's Chief Scientist

Mr. Hasson is the Chief Scientist of the Ministry of Economy of Israel since January 2011. The Office of the Chief Scientist (the “OCS”) in the Israeli Ministry of Economy is the government entity in charge of the execution of government policy for support of industrial R&D. For ten years prior to his appointment, Mr. Hasson was a general partner at Gemini Israel Funds, one of Israel's top tier Venture Capital firms.

Ms. Melissa Hathaway | President, Hathaway Global Strategies, LLC, Former Senior Director for Cyberspace at the National Security Council, USA

Ms. Hathaway, President of Hathaway Global Strategies, LLC, brings a multi-disciplinary and multi institutional perspective to strategic consulting and strategy formulation for public and private

sector clients. In the government sector, Ms. Hathaway provides strategic advice to the U.S. Government, NATO, and Interpol, as well as numerous governments around the world as they develop and refine their national strategies for cyber security. At Harvard, Ms. Hathaway is participating and contributing to the joint MIT-Harvard Project Minerva. She is contributing to the interdisciplinary research program by developing methods to measure, model, interpret and analyze challenges and responses in cyberspace. From February 2009 to August 2009, Ms. Hathaway served in the Obama Administration as Acting Senior Director for Cyberspace in the National Security Council.

Rabbi Prof. Daniel Hershkowitz | Israel's Minister of Science and Technology

The Minister of Science and Technology, mathematician, community rabbi and public figure. From 2000 to 2004 Prof. Hershkowitz, served as Dean of the Faculty of Mathematics in the Technion - Israel Institute of Technology. In addition to his academic work at the Technion, Prof. Hershkowitz also served as President of the International Linear Algebra Society (ILAS). Prof. Hershkowitz has served in many other public positions, holding membership in the Forum for National Responsibility, on the Board of Trustees at Machon Lev- The Jerusalem College of Technology, the Academic Council of the Arab Academic College in Haifa, the Governing Council of Haifa University's Center for Jewish Education, and the Steering Committee for Science and Technology Studies at the Ministry of Education.

Adv. Deborah Housen-Couriel | Yuval Ne'eman Workshop for Science, Technology and Security

Adv. Housen-Couriel is a Research Fellow at Tel Aviv University's Yuval Ne'eman Workshop for Science, Technology and Security specialising in international and Israeli cyber law and regulation. She also serves as the full-time Director of the Wexner Foundation's Israel Fellowship Program, based in Jerusalem. Between 1994 and 2005, she was Director of the Department of Regulation and International Treaties in the Israeli Ministry of Communications, and served as well in the Director-General's Bureau of the Ministry. She received her B.A. in History and Anthropology summa cum laude from Wellesley College and the Ecole de Sciences Politiques in Paris; her LL.B. and LL.M. cum laude from Hebrew University; and a M.P.A. from Harvard's Kennedy School of Government as a Wexner Foundation Fellow in 2000-2001.

Mr. Eric M. Hutchins | Fellow and the Chief Intelligence Analyst, Lockheed Martin (LM-CIRT)

Mr. Hutchins is a Lockheed Martin Fellow and the Chief Intelligence Analyst for the LM Computer Incident Response Team (LM-CIRT). This team is responsible for detecting, assessing and mitigating advanced information security threats across the corporation. Mr. Hutchins is lead innovator of novel tradecraft like the “Cyber Kill Chain™” and “Intelligence-Driven Defense™”, leveraging established DoD doctrine and tailoring it for the cyber domain. Since 2007, Mr. Hutchins has led multiple partnerships in the defense, telecom, energy, and finance sectors for cooperative threat information sharing. Mr. Hutchins is a member of the Center for Cyber Intelligence Analysis and Threat Research (CCIATR) and took his degree of Bachelors in Computer Science from the University of Virginia.

Adv. Admit Ivgi | Researcher, the Yuval Ne’eman Workshop for Science, Technology and Security.

Adv. Admit Ivgi has hands-on experience in information security through her work at RSA, the security division of EMC, as an analyst and researcher of internet fraud. She has both a technological background and experience in commercial litigation and cyber law, as well as having worked with hi-tech companies. She has degrees in law and business administration, with a specialty in international commercial law, from the Herzliya IDC.

Mr. Eugene Kaspersky | Chairman & CEO Kaspersky Lab

In 1987, Mr. Kaspersky graduated from the Institute of Cryptography, Telecommunications and Computer Science in Moscow, where he studied mathematics, cryptography and computer technology, majoring in mathematical engineering. In 1997, Mr. Kaspersky and his colleagues established Kaspersky Lab. The company is now one of the world’s top-four leading vendors of computer security software. Eugene holds a large number of national and international awards for his long track record of technological, scientific and business achievements.

Prof. Joseph Klafter | President of Tel-Aviv University

Prof. Klafter is widely recognized in his field, chemical physics. He completed his BSc and MSc in physics at Bar-Ilan University, and his PhD in chemistry at Tel Aviv University in 1978. Prof. Klafter has published close to 400 scientific articles and edited

18 books. He is a member of the editorial boards of six scientific journals, and has been a member of the scientific committee of dozens of conferences. Prof. Klafter chaired the Department of Physical Chemistry at TAU from 1990 to 1992, and again from 1998 to 2002. Concurrently he served as head of the Raymond and Beverly Sackler Institute of Chemical Physics. From 1996 to 2002 he was a member of the academic board of the Israel Science Foundation (ISF), and headed the exact sciences and technology subject area. From 2002 to 2009 he was chairman of the academic board of the ISF.

Prof. Catherine B. Lotrionte | Director, Institute for Law, Science & Global Security, Georgetown University

Prof. Lotrionte is the Director of the Institute for Law, Science and Global Security and Visiting Assistant Professor of Government and Foreign Service at Georgetown University. In 2006 she founded the CyberProject at Georgetown University under the auspices of the Institute. Through the CyberProject she organizes an annual international cyber engagement conference at Georgetown bringing together US and foreign government officials, private sector experts and academics. In 2002 she was appointed by General Brent Scowcroft to be Counsel to the President's Foreign Intelligence Advisory Board at the White House, a position she held until 2006. Prof. Lotrionte earned her Ph.D. from Georgetown University and her J.D. from New York University and is the author of numerous publications, including a forthcoming book concerning U.S. national security law in the post-Cold War era.

Mr. Yanki Margalit | Social entrepreneur, Chairman Spacell, Partner Innodo Ventures

Mr. Margalit is a social entrepreneur and speaker best known for starting Aladdin Knowledge Systems. He is currently Chairman of Spacell, a non-profit space technology organization competing for the Google Lunar X Prize and a partner in Innodo, a seed investment fund boosting Israeli startups.

Dr. Eviatar Matania | Head of the National Cyber Bureau, Prime Minister's Office

Dr. Matania is the Head of the National Cyber Bureau in the Prime Minister office of Israel. He is a graduate of the elite Talpiot program. He holds a B.Sc. (cum-laude) in Physics and Mathematics

(Hebrew University), a M.Sc.(cum-laude) in mathematics (Tel-Aviv University) with an expertise in game theory, and a Ph.D (Hebrew University) in Judgment and Decision Making. Dr. Matania brings a vast experience in the national level of R&D projects and System Analysis, as well as in the academic field of Judgment and Decision Making.

Mr. Guy Mizrahi | CEO, Cyberia

Mr. Mizrahi is the CEO and Co-Founder of Cyberia, privately owned Cyber startup. In the past Guy was the head of a cyber research team at Elbit systems, and a senior cyber consultant at IDF. Guy is hacking and information security expert well acquainted with the cyber world for more than 15 years. He is an active member of exclusive hacking forums around the world and the writer of the well-known hacking blog www.guym.co.il. Guy is also the owner of the biggest hacking community in Israel (www.hacking.org.il).

Mr. Tal Mozes | Hacktics Leader, Advisory Services, Ernst & Young

Mr. Mozes leads Ernst & Young's Advanced Security Center of Excellence (Hacktics) based in Tel Aviv, Israel. This cutting-edge red team is dedicated to cyber and information security research and consultancy for EY clients around the globe. Mr. Mozes has over fourteen years of experience in information security, as well as experience in managing and training professional information security staff, which focusing on cyber security, threat intelligence, database, infrastructure, network and application security. Mr. Mozes is also a Major in the Israeli Defense Force.

PM Benjamin Netanyahu | Prime Minister of the State of Israel

The current Prime Minister of Israel. Mr. Netanyahu also served as the prime minister of Israel from 1996-1999 and for a second term from 2009. Following his army service in the elite Sayeret Matkal unit, Netanyahu enrolled at the Massachusetts Institute of Technology, where he matriculated with a BS in Architecture. He remained at MIT for his graduate studies where he earned an MBA from the Sloan School of Management. After leaving office in 1999, Netanyahu served as a consultant for Israeli High-Tech companies. He was a highly sought-after speaker in various forums around the world and maintained a rigorous lecturing schedule. Netanyahu returned to public life in 2002 first as Foreign Minister and in 2003 as Finance Minister.

Dr. Abe Peled | Executive Chairman, NDS Group Ltd

Dr. Peled is Chairman and CEO of NDS Group Ltd, the leading provider of digital technology solutions for the pay-TV industry. Prior to joining NDS, from 1974 to 1993 Dr. Peled worked at IBM's Research Division in the United States. From 1985 to 1993, he held the position of Vice President for Systems and Software, a role in which he had management responsibility for all worldwide research and advanced development activities in these areas. Dr. Peled served as Senior Vice President for Business Development at Elron in Israel from 1993 to 1995. Dr. Peled completed both a BSc (1967) and an MSc (1971) in Electrical Engineering at the Technion Institute in Israel. He undertook graduate work at Princeton University in the United States and achieved his PhD in digital signal processing in 1974.

His Excellency Shimon Peres | President of the State of Israel

In 2007 Mr. Peres was elected to serve as the ninth President of the State of Israel. In the past, Mr. Peres served as a Member of Knesset for 48 years, the longest term of service in the history of the Israeli Knesset. He served as Minister in 12 cabinets and served twice as Prime Minister (1984-1986, 1995-1996), Deputy Minister of Defense under Ben-Gurion (1959-1965), Treasury Minister (1988-1990), Minister of Defense (1974-1977, 1995-1996), and Foreign Minister (1986-1988, 2001-2002).

Lim Chuan Poh | Chairman, National Infocomm Security Committee (NISC) and Chairman, Agency for Science, Technology and Research (A*STAR), Singapore

Mr. Lim Chuan Poh was appointed Chairman A*STAR on 1 April 2007 to lead A*STAR in conducting world-class scientific research and developing human capital for a vibrant knowledge-based, innovation-driven Singapore. Internationally, Mr. Lim Chuan Poh is a Council Member of the Science and Technology in Society (STS) forum and a Member of Japan's World Premier International (WPI) Initiative Programme Assessment and Review Committee since 2007. For his contributions in Science and Technology in Singapore, Mr Lim Chuan Poh was conferred the Honorary Degree of Doctor of Science by Loughborough University (UK) on 2008; the Honorary Degree of Doctor of Laws by Monash University (Australia) on 2009; the Fellowship of Imperial College on 2010; and the Honorary Degree of Doctor of Laws by the Arizona State University (USA) on 2012.

Dr. Thomas Rid | Reader in War Studies, King's College London

From 2006 to 2009 he worked at the School for Advanced International Studies, Johns Hopkins University, the RAND Corporation in Washington, and at the Institut français des relations internationales in Paris. Dr. Rid wrote his first book at the Stiftung Wissenschaft und Politik, Berlin's major foreign policy think tank. Dr. Rid holds a Ph.D from the Humboldt Universität zu Berlin. His numerous articles appeared in major English, French, and German peer-reviewed journals as well as magazines and newspapers. Dr. Rid has commented on current affairs on the BBC, CNN, Sky, al-Jazeera, and others.

Mr. Doron Rotem | Director, Crisis & Emergency Management Solutions, MLM Division, Systems Missiles & Space Group, Israel Aerospace Industries Ltd.

Mr. Rotem has over 30 years of experience in Communication and Information Technologies. He has managed the development of numerous Command and Control systems for both Defense and Commercial markets. As Director, Crisis & Emergency Management Solutions in IAI/MLM, Mr. Rotem is currently managing MLM's C4I, Cyber Defense and USV product lines.

Mr. Ed Schwartz | VP and CISO, RSA, the Security Division of EMC

Mr. Schwartz is Chief Information Security Officer (CISO) for RSA and has 25 years experience in the information security field. Previously, he was CSO of NetWitness (acquired by EMC), CTO of ManTech, EVP and General Manager of Global Integrity (acquired by INS), SVP of Operations of Guardent (acquired by VeriSign), CISO of Nationwide Insurance, a Senior Computer Scientist at CSC, and a Foreign Service Officer with the U.S. Dept. of State. Mr. Schwartz has advised a number of early stage security companies, and served on the Executive Committee for the Banking Information Technology Secretariat (BITS). Mr. Schwartz has a B.I.S. in Information Security Management and an M.S. in Information Technology Management from the George Mason University School of Management.

Mr. Adi Sharabani | CEO Skycure Security

Mr. Sharabani is a Global information security specialist and the CEO of a Startup Company that provides security solutions for mobile devices. Formerly, Mr. Sharabani held network security Start-up Company that was acquired by IBM in 2007. In his various roles Mr. Sharabani was responsible for the security of most IBM

software products developed around the world, led a group of IBM Research in network security, wrote numerous patents in the field and was recognized as an IBM Master Inventor.

Mr. Robert Shaw | CEO and President, Net Optics Inc.

As President and Chief Executive Officer of Net Optics since 2001, Mr. Shaw is responsible for conceiving and implementing corporate vision and strategy to position Net Optics as the leading provider of Total Application and Network Visibility solutions for both physical and virtual environments. received 2012 Best of Interop honors; received the coveted California Council for Excellence for Achieving Superior Performance and Sustainability Quality Award; 2011 Red Herring Top 100 North America Award for promise and innovation, the 2011 Best Deployment Scenario Award for Network Visibility, and many other accolades. Mr. Shaw's leadership experience spans startups to Fortune 200 organizations, where he held Senior Vice Presidential executive positions. Mr. Shaw earned both a Bachelor of Arts degree in Business and a Bachelor of Science degree in Economics from Geneva College in Pennsylvania.

Mr. Lior Tabansky | Researcher, the Yuval Ne'eman Workshop for Science, Technology and Security.

Researcher, the Yuval Ne'eman Workshop for Science, Technology and Security. Doctoral candidate, Department of Political Science, Tel Aviv University

Prof. Eran Tromer | Blavatnik School of Computer Science, Tel Aviv University

Prof. Eran Tromer is a faculty member at Tel Aviv University's School of Computer Science. His research focus is cryptography, information security, and the challenges raised by imperfect real-world computer systems. He received his PhD at the Weizmann Institute of Science, after his undergraduate degree at the Technion. Prior to joining Tel Aviv University, Prof. Tromer pursued his research at the Massachusetts Institute of Technology and at Microsoft Research. Prof. Tromer is co-heading the Check Point Institute for Information Security, and his research group is collaborating with government and industry on addressing the challenges of insecure information systems.

Dr. Roey Tzezana | Unit for Technology & Society Foresight at Tel Aviv University

Dr. Tzezana graduated at the Technion program of Nanotechnology. He is a researcher at the Unit for Technology & Society Foresight at Tel Aviv University. His research is spread across a wide variety of fields, but his main focus is on human enhancement and security. Dr. Tzezana conducts his research in collaboration with the Ministry of Defense, the Israeli Police, the Airports' Authorities, the European Union and others.

Dr. James Van de Velde | Lecturer, Center for Advanced Governmental Studies, Johns Hopkins University; Associate, Booz Allen Hamilton

Dr. Van de Velde, is a Lecturer at the Center for Advanced Governmental Studies, Johns Hopkins University (where he teaches graduate courses on intelligence and counter terrorism), has published on counter terrorism, nuclear weapons issues, drug trafficking, intelligence collection and analysis, cyber affairs and diplomatic history. He has over 20 years of experience in academia, intelligence collection and analysis, political, counter terrorism and proliferation analysis, and national security affairs. He is a former White House Appointee for nuclear weapons arms control under President George H. W. Bush, Lecturer of Political Science at Yale University, State Department Foreign Service Officer and naval intelligence reserve officer. Dr. Van de Velde received his B.A. from Yale University and his Ph.D. from the Fletcher School of Law and Diplomacy.

Mr. Eli Yitzhaki | Strategic & Business Development Leader, ELTA SIGINT EW & Communication Division

Mr. Yitzhaki is an ELTA SIGINT EW & Communication Division -Strategic & Business Development Leader. Mr. Yitzhaki retired January 2010 from the position of Vice President Advanced Initiatives for UAV Systems. Prior to this appointment, Mr. Yitzhaki was the Vice President Business development & Marketing for UAV, Security & Tactical Systems in Elbit Systems, the President and CEO of Rafael USA Inc. and had a long and successful career with the Israeli Air Force and Israeli Defense Ministry. Mr. Yitzhaki was the head of the Electronics Systems Division in the Israeli Ministry of Defense R&D agency MAFAT, where he was responsible for many innovative developments of sophisticated secured data links as well as radar, Imaging radars (SAR) and EW systems.

Conferences' Sponsorships and Associations

Yuval Ne'eman Workshop's 2nd Annual International Conference on: Cyber Security – 2012 Was Sponsored By:

To join Yuval Ne'eman Workshop for Science, Technology and Security email list send your email address to: sadna@post.tau.ac.il

Follow us on facebook
facebook

Our Home page
www.sectech.tau.ac.il

Follow us on Twitter
twitter

Isaac Ben-Israel's Blog
www.ben-israel.co.il

Conference No. 76

- * The conference is free of charge but requires registration.
- * For further details please contact fax no.03-6407198 or email sadna@post.tau.ac.il
- * Parking will be available outside campus

sponsorship:



In Association With:



Yuval Ne'eman Workshop and the National Cyber Bureau's 3rd Annual International Cyber Security Conference – Creating Cyber Ecosystems – 2013 Was Sponsored By:

TEL AVIV UNIVERSITY תל אביב

- * The conference is free of charge but requires registration.
- * Parking will be available outside campus.

Sponsored by:



In Association With:



Registration to the event
<http://sectech.tau.ac.il/en/register.cyber>
For further information:
Email: sadna@post.tau.ac.il Website: www.sectech.tau.ac.il
Tel: +972 (3) 6407193

To join Yuval Ne'eman Workshop for Science, Technology and Security email list, send your email address to: sadna@post.tau.ac.il

Follow us on Twitter
twitter

Follow us on facebook
facebook

Our Home page
www.sectech.tau.ac.il

Isaac Ben-Israel's Blog
www.ben-israel.co.il