Review: 2017 Strategic Trends in the Global Cyber Conflict

Gil Baram, Daniel Cohen, Zeev Shapira, Omri Wechsler, Nir Hight & Itzik Ben-Israel

Yuval Ne'eman Workshop for Science, Technology and Security

Blavatnik Interdisciplinary Cyber Research Center (ICRC)

Tel Aviv University

June 2018

Abstract

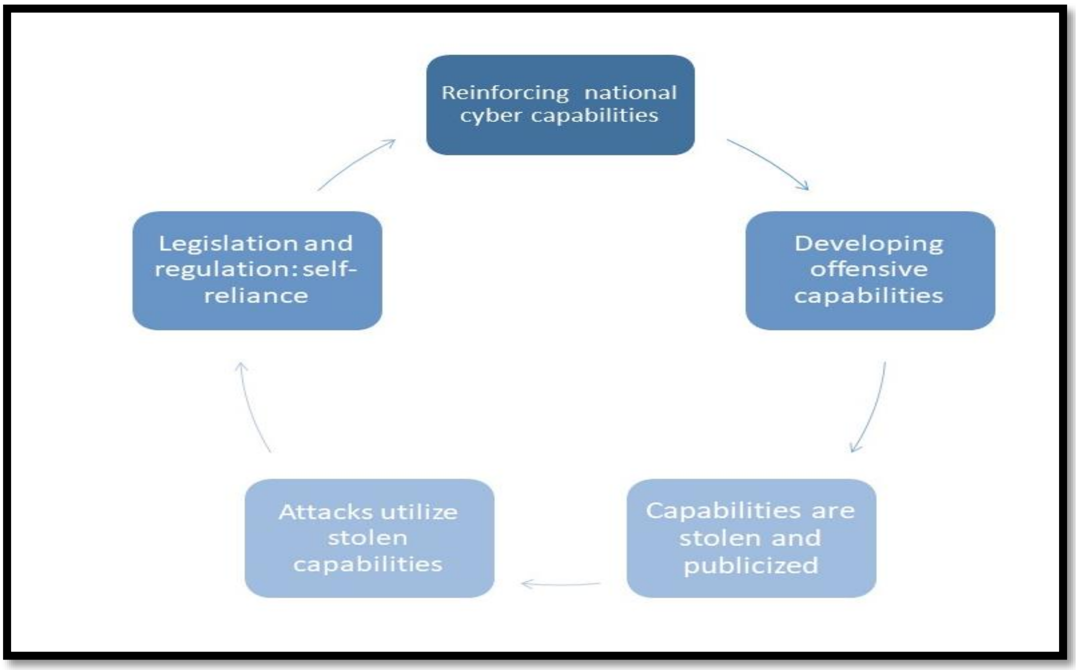
The present paper reviews the main strategic trends in cyber policy and security for 2017, pointing out the emergence of a new "Cyber Escalation Cycle:" while states are investing significant resources to improve their offensive cyber capabilities, these capabilities are subsequently being stolen, publicized and used by hostile countries to launch devastating cyber-attacks. This has led governments to pursue legislation that controls incoming technology and changes the technological relations between countries. Given the development of enhanced capabilities and the effectiveness of the attacks, we believe that leakage followed by immediate use of the leaked offensive cyber weapons against rival countries will only increase, making this issue even more contentious.

Introduction

In 2017, the global danger of cyber threats to the functioning of states, companies and societies entered both the political and public agenda, underscoring the need to defend and prepare by creating cooperation mechanisms between states and sectors. For the first time, the world experienced devastating cyber-attacks such as WannaCry and NotPetya that caused enormous damage.[1] These attacks utilized offensive tools stolen from the NSA and distributed online, and their main victims were states and large international companies. These and other attacks, in which vulnerabilities and other offensive cyber weapons were distributed and immediately utilized, exposed the slow reaction time of the attacked states, as well as a lack of cooperation and effective regulatory measures that might have prevented the massive damages.[2] Hackers have also managed to steal classified offensive cyber weapons, exploits and vulnerabilities, undermining the national security of various countries, in particular the U.S.[3]

After analyzing the main cyber policy and security strategic trends in 2017, we have identified a new phenomenon: while states are investing significant resources and making serious efforts to improve their defensive and offensive cyber capabilities, these capabilities are subsequently being stolen, publicized and used by hostile nations to launch devastating cyber-attacks. This phenomenon has led governments to pursue legislation for the control of incoming technology, and these regulatory efforts have changed the technological relations between countries. Such newly introduced measures include forcing foreign companies to allow governmental access to their data, conditioning operation within a country on source-code inspection and restricting the utilization of technological products (Figure 1).

Figure 1: The Cyber Escalation Cycle


Reinforcing national cyber capabilities
Developing offensive capabilities
Capabilities are stolen and publicized
Attacks utilize stolen capabilities
Legislation and regulation: self-reliance

Based on an analysis of the significant cyber policy and security events of 2017, we see a new process emerging. In 2017, governments and cyber protection industries set off a relatively speedy process to come up with a response to the changing reality – the cyber responsibilities of national agencies were defined, with companies following suit by adapting their security procedures. Many countries devised measures to deal with their cyber vulnerabilities, be it by re-organizing their cyber defense bodies or by addressing R&D, legislation and regulation issues. At the same time, a noticeable trend of countries imposing restrictions on incoming technologies as part of reciprocal power struggles has emerged. For example, in return for permission to introduce these products into their markets, China and Russia have been increasingly scanning source code and internal instructions for various American-made technology products; in response, the U.S. has restricted some technology imports from these countries. In addition to serving as an effective defensive measure against cyber-attacks, these restrictions and regulations are also meant to leverage cyber threats and use them to create diplomatic and political pressure.

This article is built as follows: The first section describes national investment in cyber systems and organizational changes effected in different countries. Section two describes recent public policy and offensive doctrines observed in those countries. Section three reviews the leakage of offensive tools and vulnerabilities, and the speedy utilization of leaked date for extensive attacks. Section four discusses the effects of these phenomena on the nature of the possibly evolving cyber "cold war."

Governments invest in cyber system reinforcement

In 2017, remarkable progress was made in national cyber-related strategic efforts, especially the restructuring of force buildup and reinforcement of relevant government and military branches. In May 2017, President Trump signed a presidential executive order on cyber security whose primary component was to shift responsibility for cyber-attack damages from IT personnel to the heads of federal agencies.[4] In December 2017 the U.S. Government published its national security strategy, in which it prioritizes cyber issues and the enhancement of U.S. capabilities in this field.[5] Throughout 2017, the U.S. continued its effort to convert the Cyber Command into a unified combatant command. Promoting the Cyber Command's status is perceived as a step that would guarantee its central strategic role, significantly advancing U.S. cyber capabilities apart from intelligence collection and information war.[6]

Other countries have also begun setting up cyber commands and dedicated cyber units. In China, President Xi Jingping announced a plan to establish new cyber units at the Combined Forces level, as well as opening new military cyber departments.[7] The process China is going through has been referred to as turning a big cyber power into a cyber superpower and a world-leader in this field.[8] In 2017, China characteristically developed and integrated new capabilities in its security forces and popular army, designing an ambitious ten-year plan to transform China into a global technological superpower in key technology fields, including artificial intelligence. In this context, China has announced its development of a cruise missile that would essentially rely on AI technology, in response to a similar development by the U.S. Navy scheduled for deployment in 2018.[9]

Germany has opened a new dedicated cyber command to handle imminent threats and reinforce the state's protection system. This command, headed by a general, is the sixth command of the German Army.[10] Poland has also announced its plan to set up a new cyber defense department,[11] and a military cyber warfare unit.[12] Singapore has a new cyber command that will improve coordination between military command and control networks and the growing cyber defense operations.[13] Japan's Defense Ministry announced a plan to expand its cyber defense unit from 110 to about 1,000 professionals by late 2023.[14] All of the above examples show a global phenomenon whereby nation-states - led by the U.S. - are acting to extend and strengthen their cyber commands and infrastructure, proving their recognition of the importance of addressing cyber threats in terms of national security and the need to enhance and build up their capabilities accordingly.

Cyber-attacks and reaction capabilities develop concurrently

In 2017, developments of offensive cyber capabilities were heightened, accompanied by public declarations intended to create a deterrence balance and make perpetrators pay for their actions.[15] At the beginning of his term in office, President Trump signed a secret presidential directive that enabled the U.S. government to implement a broad-ranging strategy against North Korea, including cyber warfare.[16] In several European countries, louder calls were heard to strengthen national offensive cyber capabilities. A document formulated by the governments of EU member countries (including the UK) defined cyber-attacks as acts of war, and stated that the attacked countries were allowed to retaliate using conventional weapons in accordance with their international right of self-defense.[17] The UK Defense Secretary, Sir Michael Fallon, stated that like their land, naval and air forces, the UK and its allies should further develop their cyber capabilities; such capabilities would enable the UK to retaliate by launching its own cyber-attacks.[18]

In June, Fallon warned that the UK would not hesitate to react to cyber-attacks with military force.[19] British Prime Minister Theresa May also alluded to the offensive use of cyber when she refused to rule out a cyber-attack against North Korea.[20]

In 2017, NATO acted to bolster its defensive cyber capabilities and to regulate the response to cyber-attacks against its member countries. In March, NATO's Deputy Supreme Allied Commander in Europe said that Article 5, which deals with collective response, must be expanded to include attacks against NATO members that necessitate a response by other NATO countries. He said that the distribution of misinformation and fake news must also be included in Article 5.[21] In June, NATO announced cyberspace as a legitimate military domain, triggering Article 5 in the event of cyber-attacks.[22]

France also announced its intention to adopt an offensive doctrine against cyber-attacks given Russian attempts to intervene in its democratic processes. France asserted that it would not limit its reaction to cyberspace and would also use conventional weapons.[23] The German Armed Forces announced intensification of efforts to recruit potential cyber personnel, investing some €2.6 billion in developing and training cyber experts.[24] Australia announced its cybernetic diplomacy strategy, defining the use of offensive cyber capabilities and describing its deterrence and retaliation options in case of unacceptable cyberspace conduct.[25] Canada has also acted to strengthen its cyber capabilities: in June 2017, the Canadian Defense Ministry issued a document defining the need to boost Canada's active defense and cyber-attack capabilities.[26]

Leakage of attack tools and their utilization in cyber-attacks

In 2017, the world witnessed devastating cyber-attacks utilizing attack tools developed by American intelligence agencies that were subsequently made public. In May, WannaCry caused damage to over 230,000 computers in 150 countries. A month later, the NotPetya attack damaged corporate computer systems in numerous countries, primarily Ukraine, causing huge monetary losses for the victims.[27] Consequently, the state of national preparedness and responsibility for the protection against such attacks has become part of the public agenda, with calls for urgent action. As the investigation into the WannaCry attack progressed, it turned out that the EternalBlue component (developed by the NSA to take advantage of loopholes in operation systems) had been leaked by The Shadow Brokers Group as early as April 2017; in December 2017, the U.S. accused North Korea of perpetrating the attack. The NotPetya investigation also revealed that an EternalBlue variant had been used, and in February 2018 the U.S., Britain and other countries accused Russia of the attack; they claimed that the attack was part of a Kremlin attempt to undermine Ukraine, and that Russia would bear the consequences.[28]

Moreover, in 2017 Wikileaks released an assortment of classified CIA documents as part of their Vault 7 leakage series. The documents contained information on classified projects and on the hacking of Linux and MacOS X components, as well as components used to intercept communications, regulate traffic and disable security cameras.[29] In November, Wikileaks launched the Vault 8 leakage series, publicizing the source code and development design of the Hive control server, used for remote control of malware.[30] Various reports indicated that Russian hackers managed to steal classified materials– including information on the hacking of foreign computer networks and on compromising cyber defense–by accessing the PC (installed with a Kaspersky AV software) of an NSA contractor dismissed in 2015 .[31]

These leaks exposed the U.S. intelligence agencies to criticism of their cyber protection methodologies. Hackers were fast to take advantage of leaked components prior to patch release and before different organizations updated their security definitions. The leaked attack tools were distributed instantly, facilitating their use by hackers against new targets.

These events show how processes such as strengthening cyber systems and developing national cyber offensive capabilities can turn into vulnerabilities if said capabilities are stolen and publicized - hostile elements can use these cyber tools to cause harm to countries, including the countries from which the tools were stolen in the first place.

Cold war in cyberspace?

In 2017, it became obvious that because the Internet and various communication networks are not adequately protected, a technological advantage can be gained by locating vulnerabilities in the systems of rival countries; this could facilitate a discrete operational capability to gather information, disrupt civilian life and damage critical infrastructures. Three main trends manifested the growing distrust and tension relating to the strategic cyber-attacks of 2017: 1) legislation meant to restrict privacy; 2) governmental inspection of source code; 3) restrictions on the use of technologies developed by companies in certain countries. These moves were ultimately intended to gain international advantage via diplomatic and economic means.

One salient trend in 2017 was the blocking of sites and applications that offered anonymity. The Chinese national cybersecurity law prohibiting the use of VPNs and other technologies enabling the anonymous access of sites was passed in November; this legislation prevents the access of content not approved by the government, essentially making it illegal to bypass the Great Firewall of China (GFW). China also imposed stricter censorship on news sites and network providers via rigorous legislation limiting the content of news items offered on online platforms, and requiring that all content be reviewed by a team of government-appointed editors.[32] In response, several American companies have suspended certain services and modified others. Apple took the lead, removing VPN services from its App Store in China. VPN service providers criticized this move, claiming that Apple willfully succumbed to pressure from the Chinese authorities without a fight.

Foreign companies are also concerned about the restrictions placed on their content, as it can undermine security and disclose proprietary product information by installing backdoor access. This is just one of the many challenges foreign companies have to overcome when operating in China. The 2017 law mandates foreign companies to provide the Chinese authorities source code and content access. If not, they may have to abandon the Chinese information technology market, estimated at $242 billion for 2018. So far, companies such as Microsoft, Intel and IBM have been struggling against various articles of the law, albeit unsuccessfully.[33]

In parallel with rigorous censorship and stricter regulations on privacy and state sovereignty, the mandatory scanning of source code prior to product introduction is another contentious issue causing growing tension between states; this has primarily occurred between the U.S., Russia and China. Such landmine sanctions, regulations and legislation are used by rival countries to create pressure on their adversaries. As part of its policy on technology imports, the Russian government requires source code inspection for cybersecurity products such as Firewalls and AV software to verify that they do not contain loopholes enabling access to Russian systems. In practice, however, these checks also allow Russia to explore and exploit the products' vulnerabilities. Nonetheless, many companies chose to allow the Russian authorities to inspect their products. HPE, for example, allowed the Russian authorities to inspect its protection software ArcSight, also used by the Pentagon, to introduce it into the Russian market.[34] Other firms including McAfee, Cisco and SAP said their products were being checked in external laboratories located outside Russia.[35]

In the U.S., the Trump Administration has taken a number of high-profile steps to protect both public and private sectors from Russian and Chinese interference. For example, government agencies were instructed to remove Kaspersky products from their networks in response to warnings by U.S. intelligence agencies that the company has connections with the Russian government, an accusation that Kaspersky has firmly denied;[36] following the U.S. announcement, Britain and other countries also warned against using Kaspersky products.[37]

The U.S. Congress Strategic Forces Subcommittee added a paragraph to the 2018 defense budget proposal restricting the Pentagon's purchase of technology and equipment made by the Chinese companies ZTE and Huawei - both suspected of having connections with the Chinese Army - and by Russian producers that are potential cyber threats.[38] Furthermore, the Committee on Foreign Investments in the U.S. (COFIUS) recommended against a $1.3 billion deal for the acquisition of the U.S. company Lattice Semiconductor by Canyon Bridge Capital Partners because it is partly financed by the Chinese government. President Trump subsequently signed a presidential directive banning this acquisition, claiming it may potentially cause harm to national security.[39]

Another such example was barring the acquisition of the U.S. microchip producer Qualcomm by Singapore-owned Broadcom, on the pretext of safeguarding U.S. security interests and out of concern for possible Chinese involvement that would undermine the technological leadership of the U.S.[40] The U.S. Armed Forces followed suit in prohibiting the use of drones manufactured by the Chinese company DJI, demanding the removal of all applications, media storage and batteries from all of the devices produced by that company.[41] In this context, U.S. intelligence and security agencies use of products manufactured by Beijing-based Lenovo products has been restricted for several years.[42]

This escalating distrust between the U.S., Russia and China (among others) is liable to significantly reduce cooperation in spheres that are inherently sensitive, especially cyber-related technology; this is apparent in the March 2018 trade restrictions between the U.S. and China. Growing concern about espionage and exploitation of vulnerabilities to launch cyber-attacks has resulted in an increase in regulatory measures and other tools to safeguard national sovereignty. Cyberspace also seems to have been used to create diplomatic pressure on rival countries, which are themselves suspected of launching cyber-attacks against one another.

Summary

The present paper shows how measures taken by governments to strengthen their national cyber systems and build up their cyber power has in fact led to an increase in the distribution of cyber weapons, with hostile elements stealing attack capabilities and using them to launch strategic cyber-attacks against rival countries. Countries have addressed these threats by implementing cyber and technology controls and regulations against other countries, restricting access to their systems.

Certain superpowers have been using cyberspace to create diplomatic pressure on their adversaries, and the implications of this policy are already noticeable. Tension has been growing between the U.S., Russia and China relating to source code inspection and restrictions on technologies entering Russia and China. In response, the U.S. has barred use of certain Chinese- and Russian-made products[43] by governmental and security bodies. There is concern that this "cyber arms race" will exacerbate, given: 1) the considerable resources these global powers have been investing in reinforcing defensive and offensive cyber capabilities, and 2) the deepening mistrust and suspicions between these three global powers. Given the progress and sophistication of such offensive and defensive cyber capabilities, the leakage of offensive cyber weapons and their immediate use against adversaries will only escalate in the coming years. Devising mechanisms to close the existing gap in reaction time is therefore paramount.

While historically advanced strategic technological capabilities rarely fell into hostile hands and such incidents were covered up, stolen capabilities are now immediately publicized and in short order translated into cyber-attacks. Moreover, once these capabilities are exposed and explored, a process begins whereby the "cost" of developing cyber weapons goes down, as there is growing evidence that such cyber-attack tools are being produced and offered on the "black market" run by cyber criminals. The manifestation of cyber weapon is being used as a pretext for issuing regulations to block off foreign companies, thus putting de facto diplomatic pressure on the involved companies' countries of origin.

This begs the question as to whether responsibility for the risks those companies are exposed to falls on their countries of origin. Indeed, if the U.S. were to demand inspecting the source codes of Russian and Chinese technologies, this could lead to mutual deterrence similar that which existed between the U.S. and the Soviet Union in the Cold War era. Such a solution, however, can only be piecemeal, since smaller and weaker countries are not in a position to confront the superpowers with such a demand. Even though it is only an interim solution, signing agreements to normalize the situation promises to improve the (unacceptable) current reality whereby state-sponsored offensive tools are distributed online and used to perpetrate large-scale attacks. This kind of response would have two additional advantages: 1) it would impose an economic cost on the involved parties, and 2) it would promote a process for defining cyber sovereignty borders between countries.

In recent decades, numerous countries have recognized that the challenges of cyberspace are at the core of their national and international interests. They began developing new strategies, setting up dedicated organizations and incorporating specific regulations in the cyber domain. However, while those states have acted upon the assumption that in future clashes they would use kinetic power in addition to cyber warfare, in 2017 it became apparent that to attain their cyber security goals, they must define new behavioral norms and formulate legal tools through international cooperation.

References

[1] In late June, the Danish shipping giant Maersk reported massive jams caused by the NotPetya attack in 76 ports where the company operates in the U.S., India, Spain and the Netherlands, resulting in delays and other problems in cargo shipment. In August, Maersk announced that the attack damage amounted to $200-300 million. Oded Yaron. "Shipping Giant: Cyber-attack may cause a $300 million loss". *HaAretz*, August 17, 2017. https://www.haaretz.co.il/captain/net/1.4364426, accessed March 23, 2018; Teis Jensen. "Cyber-attack Hits Shipper Maersk, Causes Cargo Delays." *Reuters*, June 28, 2017. https://www.reuters.com/article/us-cyber-attack-maersk/maersk-says-working-on-recovery-plan-after-cyber-attack-idUSKBN19J0QB. Accessed March 7, 2018.

[2] See, for example, Max Smeets, "A matter of time: On the transitory nature of cyberweapons". *Journal of Strategic Studies*, 2017: 1-28. https://doi.org/10.1080/01402390.2017.1288107.

[3]On the effect of cyber weapon proliferation see Adam Liff, "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war". *Journal of Strategic Studies*, *35*(3), 2012: 401-428. https://doi.org/10.1080/01402390.2012.663252. On the use of offensive cyber weapons see, for example, Dale Peterson, "Offensive cyber weapons: construction, development, and employment." *Journal of Strategic Studies*, *36*(1), 2013: 120-124. https://doi.org/10.1080/01402390.2012.742014.

[4] Joe Uchill. "Trump Signs Cybersecurity Executive Order." *The Hill*, May 11, 2017. Accessed Mar 2, 2018. http://thehill.com/policy/cybersecurity/332968-trump-signs-cybersecurity-executive-order

[5] Morgan Chalfant. "Trump's National Security Strategy Calls Out Russia for 'offensive Cyber Efforts'. *"The Hill*, December 18, 2017. Accessed Mar 29, 2018. http://thehill.com/policy/cybersecurity/365462-trumps-national-security-strategy-calls-out-russia-for-offensive-cyber.

[6] Partrick Tucker. "What the Announced NSA / Cyber Command Split Means." *DefensOne*, August 18, 2017. Accessed Mar 29, 2018. http://www.defenseone.com/technology/2017/08/what-announced-nsa-cyber-command-split-means/140362/ .

[7] Tom O'Connor. "Chinese Military Begins Massive Reforms for an 'Indestructible Combat Force'." *NewsWeek*, April 19, 2017. Accessed Mar 29, 2018. http://www.newsweek.com/chinese-military-prepares-massive-changes-new-cyber-division-586313

[8] Adam Segal. "Year in Review: Chinese Cyber Sovereignty in Action." *Council on Foreign Relations*, January 8, 2018. Accessed Mar 9, 2018. https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action.

[9] John Markoff and Matthew Rosenberg. "China's Intelligent Weaponry Gets Smarter." *New York Times*, February 3, 2017. Accessed Mar 29, 2018. https://www.nytimes.com/2017/02/03/technology/artificial-intelligence-china-united-states.html.

[10] "German Military to Unveil New Cyber Command as Threats Grow." *Reuters*, March 30, 2017. Accessed Mar 29, 2018. https://www.reuters.com/article/us-germany-military-cyber/german-military-to-unveil-new-cyber-command-as-threats-grow-idUSKBN1712MW

[11] "Polish PM to Set Up New Cybersecurity Department." October 9, 2017. Accessed Mar 2, 2018. http://thenews.pl/1/9/Artykul/329562,Polish-PM-to-set-up-new-cybersecurity-department

[12] "New 'cyber Army' for Poland." *Radio Poland*, October 9, 2017. Accessed Mar 29, 2018. http://thenews.pl/1/9/Artykul/329648,New-'cyber-army'-for-Poland.

[13] Kelvin Wong. "Singapore integrates C4 and cyber defence operations with new command*", Jane's International Defence Review*, July 4, 2017. Accessed Mar 29, 2018. http://www.janes.com/article/71987/singapore-integrates-c4-and-cyber-defence-operations-with-new-command

[14] "Defense Ministry Plans to Boost Strength of Unit Tasked with Countering Cyberattacks." *The Japan Times Online*, July 17, 2017. https://www.japantimes.co.jp/news/2017/07/17/national/politics-diplomacy/defense-ministry-plans-boost-strength-unit-tasked-countering-cyberattacks/?utm_content=buffer8df0c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

[15] Sean Carberry. "House Adds Cyber Strategy Provision to Defense Bill." *FWC*, July 14, 2017. Accessed Mar 29, 2018. https://fcw.com/articles/2017/07/14/ndaa-cyber-carberry.aspx.

Various researchers have questioned the feasibility of cyber deterrence, given that the opponent is often unknown, nor is the best way to deter him (Libicki, 2009). Fischerkeller & Harknett (2017) claim that deterrence is not as important in cyberspace, and no state may rely on deterrence in its defense strategy. Nye (2017) assesses that cyberspace is essentially civilian rather than military, with a dynamic that is different from that of the traditional military sphere. Draw a parallel between Cold War deterrence and cyber deterrence is difficult.

For the ongoing debate on the meaning of cyber deterrence and whether countries are able to achieve it, see: Will Goodman," Cyber deterrence: Tougher in theory than in practice?", *Strategic Studies Quarterly*, *4*(3), 2010: 102-135. https://search.proquest.com/docview/1430516879?accountid=14765;Richard j. Harknett & Joseph S. Nye, "Is deterrence possible in cyberspace?" *International Security*, *42*(2), 2017: 196-199. https://doi.org/10.1162/ISEC_c_00290 ; Joseph S. Nye, "Deterrence and dissuasion in cyber." *International Security*, *41*(3), 2017: 44-71. https://doi.org/10.1162/ISEC_a_00266; Martin C. Libicki, *Cyberdeterrence and cyberwar*. 2009: Rand Corporation., Santa Monica. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

[16] Karen DeYoung, Ellen Nakashima, and Emily Rauhala. "Trump Signed Presidential Directive Ordering Actions to Pressure North Korea." *Washington Post*, September 30, 2017. https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html.

[17] James Crisp. "EU Governments to Warn Cyber-attacks can be an Act of War." *The Telegraph*, October 29, 2017. Accessed Mar 9, 2018. https://www.telegraph.co.uk/news/2017/10/29/eu-governments-warn-cyber-attacks-can-act-war/. ; The Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.

[18] Ben Farmer. "Britain could Carry Out Cyber-attacks to Defend Itself Against Russia, Suggests Sir Michael Fallon." *The Telegraph*, February 2, 2017. https://www.telegraph.co.uk/news/2017/02/02/britain-could-carry-cyber-attacks-defend-against-russia-suggests/ ; Steve Ranger. "Russian Hackers Target Critical Infrastructure and Democracy, Warns UK." *Znet*, February 3, 2017. Accessed Mar 29, 2018. http://www.zdnet.com/article/russian-hackers-target-critical-infrastructure-and-democracy-warns-uk/.

[19] Andrew Griffin. "The Government is Planning to Drop Bombs on Hackers." *The Independent*, June 28, 2017. Accessed Mar 29, 2018. http://www.independent.co.uk/life-style/gadgets-and-tech/news/petya-cyber-attack-uk-government-bombing-hackers-ransomware-wannacry-defence-michael-fallon-a7811516.html. ; "Iran Blamed for Parliament Cyber-Attack." *BBC*, October 14, 2017. Accessed Mar 29, 2018. http://www.bbc.com/news/uk-41622903.

[20] Gordon Rayner. "Theresa may Refuses to Rule Out Military Action and Cyber-attacks Over North Korea Missile Launches." *The Telegraph*, August 30, 2017. Accessed Mar 9, 2018. https://www.telegraph.co.uk/news/2017/08/29/britain-calls-sanctions-north-korea-wake-missile-test/.

[21] "British NATO General Wants Cyber-Attacks to Trigger Article 5 Collective Response." *RT*, March 5, 2017. Accessed Mar 29, 2018. https://www.rt.com/uk/379371-nato-cyber-attack-war/.

[22] Phil Muncaster. "Nato Confirms Cyber as Legitimate Military Domain." June 29, 2017. Accessed Mar 9, 2018. https://www.infosecurity-magazine.com:443/news/nato-confirms-cyber-legitimate/.

[23] Henry Samuel. "Emmanuel Macron Prepared to use Force to Retaliate Over Russian Cyber-attacks, Top Aide Suggests." *The Telegraph*, May 8, 2017. Accessed Mar 9, 2018. https://www.telegraph.co.uk/news/2017/05/08/emmanuel-macron-prepared-use-force-retaliate-russian-cyber-attacks/

[24] Derek Scally. "We'll Fight them on the Internet: Germany's First Cyber General." *Irish Times*, April 8, 2017. Accessed Mar 29, 2018. https://www.irishtimes.com/news/world/europe/we-ll-fight-them-on-the-internet-germany-s-first-cyber-general-1.3039196.

[25] Mike Blanchfield. "Defence Plan Calls for Cyber and Drone Attacks to Meet 21st Century Threats." *CTVNews*, June 7, 2017. Accessed Mar 29, 2018. https://www.ctvnews.ca/politics/defence-plan-calls-for-cyber-and-drone-attacks-to-meet-21st-century-threats-1.3447763.

[26] Stilgherrian. "Australia Goes Hawk with New Diplomatic Cyber Strategy." *ZNet*, October 4, 2017. Accessed Mar 29, 2018. http://www.zdnet.com/article/australia-goes-hawk-with-new-diplomatic-cyber-strategy/.

[27] Zeljka Zorz, "NotPetya aftermath: Companies lost hundreds of millions." Helpnetsecurity, August 17, 2017. Accessed Mar 2, 2018. https://www.helpnetsecurity.com/2017/08/17/notpetya-losses/

[28] Asha McLean. "Australia also Points Finger at Russia for NotPetya." *Zdnet*, February 15, 2018. Accessed Mar 2, 2018. http://www.zdnet.com/article/australia-also-points-finger-at-russia-for-notpetya

[29] Pierluigi Paganini. "Wikileaks – CIA Developed OutlawCountry Malware to Hack Linux Systems." *Security Affairs*, July 1, 2017. Accessed Mar 29, 2018. https://securityaffairs.co/wordpress/60584/breaking-news/cia-outlawcountry-hack-linux.html. ; Sooraj Shah. "WikiLeaks Reveals CIA Tool Acting as SMS Proxy on Android." *Infosecurity*, July 14, 2017. Accessed Mar 3, 2018. https://www.infosecurity-magazine.com/news/wikileaks-highrise-cia-android/.

[30] Swati Khandelwal. "Vault 8: WikiLeaks Releases Source Code for Hive - CIA's Malware Control System." *The Hacker News*, November 9, 2017. Accessed Mar 29, 2018. https://thehackernews.com/2017/11/cia-hive-malware-code.html.

[31] Dustin Volz and Joseph Menn. "Russian Hackers Stole U.S. Cyber Secrets from NSA: Media Reports." *Reuters*, October 5, 2017. Accessed Mar 3, 2018. https://www.reuters.com/article/us-usa-cyber-nsa/russian-hackers-get-u-s-cyber-defense-details-from-nsa-wsj-idUSKBN1CA2DO.

[32] Christian Shepherd and Robert Birsel. "China Tightens Rules on Online News, Network Providers." *Reuters*, May 2, 2017. Accessed Mar 29, 2018. https://www.reuters.com/article/us-china-internet-censorship-security/china-tightens-rules-on-online-news-network-providers-idUSKBN17Y0Y6.

[33] Catalin Cimpanu. "Chinese Agency Linked to Cyber-Espionage Operations Will Review Source Code of Foreign Firms." *BleepingComputer*, September 1, 2017. Accessed Mar 2, 2018. https://www.bleepingcomputer.com/news/government/chinese-agency-linked-to-cyber-espionage-operations-will-review-source-code-of-foreign-firms/
WTO's technical barriers to trade committee. Yonhap. "Korea Raises Concerns Over China's Cyber Security Measures in WTO Meeting." *Korea Herald*, November 13, 2017. Accessed Mar 29, 2018. http://www.koreaherald.com/view.php?ud=20171113000578. ; Tom Miles. "U.S. Asks China Not to Enforce Cyber Security Law." *Reuters*, September 26, 2017. Accessed Mar 9, 2018. https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-tells-wto-concerned-about-chinese-cyber-security-laws-idUSKCN1C11D1.

[34] Dustin Volz. "Foreign Government Code Reviews 'Problematic': White House Cyber." *Reuters*, October 3, 2017. Accessed Mar 29, 2018. https://www.reuters.com/article/us-usa-cyber-russia/foreign-government-code-reviews-problematic-top-white-house-cyber-official-idUSKCN1C829R.

[35] Russian Demands to Share Cyber Secrets." *Reuters*, June 23, 2017. Accessed Mar 3, 2018. https://www.reuters.com/article/us-usa-russia-tech-insight/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB.

[36] Dustin Volz. "Trump Administration Orders Purge of Kaspersky Products from U.S. Government." *Reuters*, September 13, 2017. Accessed Mar 28, 2018. https://uk.reuters.com/article/us-usa-security-kaspersky/trump-administration-orders-purge-of-kaspersky-products-from-u-s-government-idUKKCN1BO2CH.

[37] Mark Hosenball, Kanishka Singh and Costas Pitas. "UK Cyber Agency Targets Kaspersky in Warning on Russian Software." *Reuters*, December 2, 2017. Accessed Mar 3, 2018. https://www.reuters.com/article/us-kaspersky-cyber-britain/uk-bans-kaspersky-software-from-departments-responsible-for-national-security-ft-idUSKBN1DV63S. Andrius Sytas. "Lithuania Bans Kaspersky Lab Software on Sensitive Computers." *Reuters*, December 21, 2017. Accessed Mar 29, 2018. https://www.reuters.com/article/us-lithuania-russia/lithuania-bans-kaspersky-lab-software-on-sensitive-computers-idUSKBN1EF23M

[38] Bill Gertz. "House Bill Set to Restrict Pentagon from Buying Chinese Or Russian Tech Over Cyberattack Fears." *Business Insider*, June 24, 2017. Accessed Mar 29, 2018. http://uk.businessinsider.com/chinese-russian-telecommunications-devices-cyberattacks-2017-6.

[39] Liana Baker. "Trump Bars Chinese-Backed Firm from Buying U.S. Chipmaker Lattice." *Reuters*, September 13, 2017. Accessed Mar 29, 2018. https://www.reuters.com/article/us-lattice-m-a-canyonbridge-trump/trump-bars-chinese-firm-from-buying-u-s-chipmaker-lattice-idUSKCN1BO2ME.

[40] Chloe Aiello. "Trump Blocks Broadcom-Qualcomm Deal, Citing National Security Concerns." March 12, 2017. *CNBC*, Accessed Mar 29, 2018. https://www.cnbc.com/2018/03/12/trump-issues-order-prohibiting-broadcoms-bid-to-take-over-qualcomm.html.

[41] Ben Watson. "The US Army Just Ordered Soldiers to Stop using Drones from China's DJI." *DefenseOne*, August 4, 2017. Accessed Mar 3, 2018. http://www.defenseone.com/technology/2017/08/us-army-just-ordered-soldiers-stop-using-drones-chinas-dji/139999/.

[42] Hayley Tsukayama and Dan Lamothe. "How an Email Sparked a Squabble Over Chinese-Owned Lenovo's Role at Pentagon." *The Washington Post*, April 22, 2017. Accessed Mar 29, 2018. https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html