2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Offensive Cyber Capabilities: To What Ends?

Max Smeets
Center for International Security
and Cooperation
Stanford University
Stanford, United States
mwsmeets@stanford.edu

Herbert S. Lin
Center for International Security
and Cooperation
The Hoover Institution
Stanford University
Stanford, United States
herbert.s.lin@stanford.edu

Abstract: There is a growing interest in the use of offensive cyber capabilities (OCC) among states. Despite the growing interest in these capabilities, little is still known about the nature of OCC as a tool of the state. This research therefore aims to understand if (and how) offensive cyber capabilities have the potential to change the role of military power. Drawing on a wide range of cases, we argue that these capabilities can alter the manner in which states use their military power strategically in at least four ways. OCC are not particularly effective in *deterring* adversary military action, except when threatened to be used by states with a credible reputation. However, they do have value in *compellence*. Unlike conventional capabilities, the effects of offensive cyber operations do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face thus deescalating conflict. The potential to control the reversibility of effect of an OCC by the attacker may also encourage compliance. OCC also contribute to the use of force for *defensive* purposes, as it could provide both a preemptive as well as preventive strike option. Finally, its symbolic value as a 'prestige weapon' to enhance 'swaggering' remains unclear, due to its largely non-material ontology and transitory nature.

Keywords: *offensive cyber capabilities, compellence, defense, deterrence, military power, swaggering*

1. INTRODUCTION

There is a growing interest in the use of offensive cyber capabilities (OCC) among states. A diverse group of states across the world including Belgium, Columbia, Germany, Finland, India, the United Arab Emirates (UAE) and Vietnam have all said they are exploring options for cyber warfare.[1] In turn, there are signs that the states such as the United States, China, Russia, Israel, the United Kingdom, Iran and North Korea continue to further develop their offensive cyber capabilities.[2] Concurrently, many states have adopted cyberspace as a new operational domain of warfare, alongside land, air, space and sea.[3] Also NATO, following the Warsaw Summit, has acknowledged cyberspace as a military domain.[4]

Despite the growing interest in these capabilities, little is known about how states use (or expect to use) OCC to further their national goals. In a recently published report, former US Secretary of Defense, Ashton Carter, expressed his disappointment in the 'cyber component' of US efforts to destroy ISIS.[5] The report highlights an important

[1] This is not a comprehensive list of newcomers. On Germany see: Nina Werkhäuser, "German army launches new cyber command", *DW*, (April 1, 2017). Retrieved from: http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517; on Finland see: Secretariat of the Security Committee, "Finland's Cyber Security Strategy", (2013). Retrieved from: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf; on Vietnam see: Jim Dao, Giang The Huong Tran and Tu Ngoc Trinh, "New Law on Cyber Security in Vietnam", *Tilleke & Gibbins* (2016, June 3). Retrieved from: http://www.tilleke.com/resources/new-law-cyber-security-vietnam; on India see: Vivek Raghuvanshi, "New Indian Cyber Command Urged Following Recent Attacks", *Defense News*, (2016, June 6). Retrieved from: https://www.defensenews.com/2016/06/06/new-indian-cyber-command-urged-following-recent-attacks/; on United Arab Emirates see: Bindiya Thomas, "UAE Military To Set Up Cyber Command", (2014, September 30), *DefenseWorld*. Retrieved from: http://www.defenseworld.net/news/11185/ UAE_Military_To_Set_Up_Cyber_Command#.WW4nJYjyiUk; on Turkey see: Israel Defense, "Turkey Launched Cyber Warfare Command", (2014, April 13). Retrieved from: http://www.israeldefense.co.il/en/content/turkey-launched-cyber-warfare-command; on Columbia see: Christoffer Frendesen "Colombia sends officials to Estonia for cyber defense training", *Columbia Reports*, (2014, September 2). Retrieved from: http://colombiareports.com/colombias-govt-sends-security-forces-estonia-cyber-defense-training/.

[2] On Russia see: Eugene Gerden, "Russia to spend $250m strengthening cyber-offensive capabilities", *SC Magazine UK*, (2016, February 4). Retrieved from: http://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive- capabilities/article/470733; on the United States see Sean Lyngaas, "Pentagon Chief: 2017 budget includes $7Bn for cyber", *FCW* (February 2, 2016). Retrieved from: https://fcw.com/articles/2016/02/02/dod-budget-cyber.aspx; on Iran see: Bozorgmehr Sharafedin, "Iran to expand military spending, develop missiles", *Reuters*, (January 9, 2017). Retrieved from: https://www.reuters.com/article/us-iran-military-plan/iran-to-expand-military-spending-develop-missiles-idUSKBN14T15L; on North Korea see: David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More", *The New York Times* (October 15, 2017). Retrieved from: https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

[3] For a critical analysis on this branding see: Chris McGuffin and Paul Mitchell, "On domains: Cyber and the practice of warfare", *International Journal*, 69:3 (2014):394-412 .

[4] NATO CCD COE, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit", (2016, July 21). Retrieved from: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

[5] At the inaugural US Cyber Command Symposium, a more positive view of the US cyber operations against ISIS was provided. As one senior policymaker stated: "We are hitting every target, every time". Ashton Carter, "A Lasting Defeat: The Campaign to Destroy ISIS", *Report*, Belfer Center for Science and International Affairs, Harvard Kennedy School, (October, 2017). Retrieved from: https://www.belfercenter.org/LastingDefeat; Max Smeets, "US Cyber Command: An Assiduous Actor, Not a Warmongering Bully", *The Cipher Brief*, (March 4, 2018). Retrieved from: https://www.thecipherbrief.com/us-cyber-command-assiduous-actor-not-warmongering-bully.

set of issues. It rings alarm bells about the current organizational efforts of US Cyber Command.[6] It confirms findings of several scholars that the development of effective cyber capability is by no means an easy feat.[7] It also reveals the importance of contextualizing the US Cyber Command within a larger organizational structure, each component of which has its own institutional interests. Finally, Carter's statement suggests that these capabilities, even though they are very malleable and refer to a broad category of tools, may not be equally valuable in all situations against all types of actors.

The former Secretary of Defense is of course not the first senior policy maker to note disquiet about cyber weapons. In 2012, when Keith Alexander was still heading the NSA and US Cyber Command, he stated that there is "much uncharted territory in the world of cyber-policy, law and doctrine".[8] More recently, referring to Herman Kahn's classic 1959 text on nuclear strategic concepts, Michael Hayden states that "[n]o one has yet begun to write the On Thermonuclear War for cyber conflict".[9]

The purpose of this paper is therefore to explore the following question: *How and to what extent, if any, do offensive cyber capabilities have the potential to affect the roles of military power?* We do not intend to provide a highly detailed policy prescription, nor a detailed description of the requirements for the military to conduct a specific operation. Instead, this paper deals with the basic principles and aims to parsimoniously capture which goals can be realized through the use of OCC. After all, as military theorist Charles Ardant du Picq noted in the mid-19th century, "[t]he instruments of battle are valuable only if one knows how to use them".[10] As a starting point of our analysis, we use the framework developed by Robert J. Art almost four decades ago on the ends of military power. Art distinguished between four strategic roles that force can serve: i) defense, ii) deterrence, iii) compellence and iv) 'swaggering'.[11]

Our central claim is that OCC can alter the manner in which states use their military power. Offensive cyber capabilities are not particularly effective in *deterring* adversary military action, except when threatened to be used by states with a credible

[6] "I was largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques. When CYBERCOM did produce something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection. This would be understandable if we had been getting a steady stream of actionable intel, but we weren't. The State Department, for its part, was unable to cut through the thicket of diplomatic issues involved in working through the host of foreign services that constitute the Internet. In short, none of our agencies showed very well in the cyber fight".

[7] Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, 22: 3 (2013)365-404.

[8] Keith Alexander, US Senate, Committee on Armed Services, (2014, April). Retrieved from: http://www.eweek.com/security/nsa-director-says-cyber-command-not-trying-to-militarize-cyberspace.

[9] Michael Hayden, *Playing the Edge: American Intelligence in the Age of Terror*, (New York: Penguin Press: 2014).

[10] Charles Ardant du Picq, *Battle Studies: Ancient and Modern Battle*, trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

[11] The categories selected by Art are not analytically exhaustive. The categories are described in more detail below. Robert J. Art, "To What Ends Military Power?", *International Security*, 4:4 (1980)3-35.

reputation. However, offensive cyber capabilities do have value in *compellence*. Unlike conventional capabilities, the effects of OCC do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face thus deescalating conflict. The potential opportunity for the attacker to control the reversibility of effect of an OCC may also encourage compliance. At the same time, the use of OCC has escalatory potential. Cyber capabilities also contribute to the use of force for *defensive* purposes, as it could provide both a preemptive as well as preventive strike option. Finally, its symbolic value as a 'prestige weapon' to enhance 'swaggering' remains unclear, due to its largely non-material ontology and transitory nature.

The remainder of this paper consists of three parts. A study on the unique value of cyber capabilities has to start with an analysis of its distinct features. The next section therefore briefly discusses the 'rise' of OCC and assesses its characteristics. Section III, in turn, lays out the four possible functions of cyber capabilities as a tool for the state. The final section concludes and considers the implications of these findings.

2. THE RISE OF OFFENSIVE CYBER CAPABILITIES

The term 'offensive cyber capability' can have a host of different meanings.[12] We define OCC as "a capability designed to access a computer system or network to damage or harm living or material entities".[13] Adopting this definition, it also means that we exclude espionage, information warfare and information operations from our analysis. OCC encompasses a wide range of capabilities. Indeed, the cyber means used against the Ukrainian regional electricity distribution company in December 2015 are very different to those used in the DDoS attacks that swamped websites of various Estonian organizations in April 2007.[14] Rather than compile an exhaustive list of purposes and examples, we have selected three categories based on the damage

[12] This is partially because the prefix 'cyber' acts like a sponge absorbing meaning. See: James Shires and Max Smeets, "The Word Cyber Now Means Everything—and Nothing At All", *Slate*, (December 1, 2017). Retrieved from: http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_lost_all_meaning.html.

[13] Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons", *Journal of Strategic Studies*, (2017)1-28; For alternative definitions see: Thomas Rid and Peter McBurney, "Cyberweapons", *The RUSI Journal*, 157:1 (2012):6-13, p. 7; Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons", *The Journal of Information Warfare*, 13:1(2014) ; Dale Peterson. "Offensive Cyber Weapons: Construction, Development and Employment", *Journal of Strategic Studies*, 36:1(2013).

[14] A detailed analysis of each case goes beyond the scope of this paper. For an excellent overview on Ukraine see: Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack", *Wired*, (20 January 2016). Retrieved from: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/; Kaspersky Lab's Global Research & Analysis Team, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents", Securelist, (28 January 2016). Retrieved from: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, (3 March 2016). Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/;E-ISAC, SANS ICS. "Analysis of the Cyber Attack on the Ukrainian Power Grid" March 18, 2016, 4. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

caused by an OCC: denial of service, file damage and physical damage.[15] Table 1 provides an overview of some of the most important cases reported by a reputable cyber security firm.

TABLE 1. IMPORTANT INSTANCES OF OCC

Denial of Service		File Damage		Physical Damage	
Name	**Year***	**Name**	**Year***	**Name**	**Year***
Estonian DDoS attacks	2007	Witty Worm	2004	Stuxnet	2010
Hacking Scientology	2008	Dozer	2009	Ukraine attacks	2015
Georgian attacks	2009	Koredos	2010		
Black DDoS	2010	Shamoon	2012		
OPI Israel	2012	Groovemonitor	2012		
		Jokra / Dark Seoul	2013		
		Destover / Sony	2014		
		Shamoon 2.0	2016		
		NotPetya	2017		

* We listed year of disclosure rather than year of compromise. **The table does not include cases of which there is no public cyber security report available, like Sands Casino in 2014.

The deployment and use of OCCs is generally extended over multiple stages. It is common to distinguish between the following four stages for advanced operations: i) reconnaissance; ii) intrusion; iii) privilege escalation; and iv) payload delivery.[16] These stages can be explained through a simple analogy of a burglar trying to get into a house. The burglar first scans the neighborhood and sees which security measures (camera system, dog, locks) the homeowner has taken (reconnaissance). The burglar then tries to get in, normally taking the path of least resistance (intrusion). When entering a specific room, they try to gain access to other rooms and hope to find the cabinet with all the keys to the cars, vault etc. (privilege escalation). Finally, the burglar decides what to do with the obtained level of access. They may not only steal the belongings of the homeowner, but also move or destroy some of the furniture in the house. Considering these stages reveals that there are close similarities between OCC and cyber espionage capabilities or, in intelligence jargon, Computer Network

[15] These categories were adopted from: Steven M. Bellovin, Susan Landau and Herbert S. Lin, "Limiting the undesired impact of cyber weapons: technical requirements and policy implications", *Journal of Cybersecurity*, 3:1 (2017)59–68.

[16] For example, see: FireEye, "Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks", *WhitePaper*, (2012). Retrieved from: http://www.softbox.co.uk/pub/ fireeye- advanced-targeted-attacks.pdf; S. Mathew, R. Giomundo, S. Upadyaya, M. Sudit and A. Stotz, "Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams," *VizSEC '06, Proceedings of the 3rd International Workshop on Visualization for Computer Security* (2016)1-6.

Exploitation (CNE) and Computer Network Attack (CNA). Indeed, it is often said that there is no other weapon so strongly anchored in intelligence as cyber weapons.[17]

3. THE USES OF CYBER FORCE

Having developed a better understanding of the nature of OCC, we can now turn to potential function of these capabilities. Numerous works in security studies have been devoted to the use of force. We used the classic study of Robert J. Art – *To What Ends Military Power?* – as a starting point for our analysis. Art distinguishes between four categories that force can serve: defense, deterrence, compellence and 'swaggering'.[18]

A. Defense

The defensive use of military force serves to do two things: avert an attack or minimize damage of an attack. As Art states:

> "[f]or defensive purposes, a state will direct its forces against those of a potential or actual attacker, but not against his unarmed population. For defensive purposes, a state can deploy its forces in place prior to an attack, use them after an attack has occurred to repel it, or strike first if it believes that an attack upon it is imminent or inevitable".[19]

We commonly distinguish between a preemptive and preventive strike. A preemptive strike is when a state believes an attack upon it is imminent by an adversary. A preventive strike is when an attack is perceived to be inevitable but not imminent or known to be planned.[20]

Two prominent cases of preventive strikes in the late Cold War include Operation Scorch Sword, an airstrike by the Iranian air force in September 1980 that damaged an almost-complete nuclear reactor near Baghdad, Iraq and Operation Opera, the more successful bombing by the Israeli air force of the same nuclear reactor, almost a

[17] This in turn leads to an important set of questions surrounding the organizational integration of intelligence and military capabilities. See: Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks", 9th International Conference on Cyber Conflict, (Tallinn: NATO CCD COE Publications: 2017); Hayden, *Playing the Edge*.

[18] In practice, these categories are expected to overlap and may not always be easily disentangled. Also, unlike Art, we do not explicitly distinguish between the physical and peaceful use of military power. Art, "To What Ends Military Power?".

[19] Ibid. Though note that even for offensive purposes, states are prohibited from attacking unarmed populations.

[20] For an excellent overview on the need to legitimize preventive and pre-emptive use of force see: Tom Sauer, "The Preventive and Pre-Emptive Use of Force: To be Legitimized or to be De-Legitimized?" The Hoover Institution. Retrieved from: http://www.ethical-perspectives.be/viewpic.php?TABLE=EP&ID=493.

year later. Stuxnet can be similarly described as a preventive strike.[21] As Kim Zetter notes, in the lead up to the cyber attack, technicians at Natanz had begun to install new centrifuges again at a rapid rate and with their performance improving.[22] Stuxnet was presented as an 'extra option' to President George W. Bush, as Sanger notes, to effectively deal with a seemingly escalating situation, especially in the eyes of the Israeli government.[23] Stuxnet was a masterpiece of work, "[b]ut Stuxnet might only have been the beginning", as Ben Buchanan notes.[24] Indeed, there was also an option developed for a large scale pre-emptive strike. In case the situation in Iran worsened, the United States had a contingency planned, reportedly code-named NITRO ZEUS. As *The New York Times* reported:

> "Nitro Zeus was part of an effort to assure President Obama that he had alternatives, short of a full-scale war, if Iran lashed out at the United States or its allies in the region. […] [T]he plan […] was devised to disable Iran's air defenses, communications systems and crucial parts of its power grid and was shelved, at least for the foreseeable future, after the nuclear deal struck between Iran and six other nations last summer [2016] was fulfilled".[25]

Although NITRO ZEUS is the only pre-emptive cyber strike option known to date, it is likely that military forces have considered the use of OCC in this manner for other situations as well, albeit on a more modest scale. Indeed, the use of a cyber capability to, for instance, neutralize the launch of an operational ballistic missile is conceivable.

B. Deterrence

The deterrent use of military force aims to dissuade an adversary from doing something by threatening him with unacceptable punishment if he does it. Deterrence hinges upon the credible threat of retaliation to dissuade an enemy from attacking. As Bernard Brodie wrote in 1958, a credible deterrent, "must be always at the ready, yet

[21] Ralph Langner indicates that Stuxnet is actually not one weapon, but two. The earliest version, also referred to as Stuxnet 0.5, was in development prior to November 2005. This early version is considered to be the most sophisticated of the two, focusing on the closing the isolation valves of the Natanz uranium enrichment facility. The latter, better-known version followed a different modus operandi as it aimed to change the speeds of the rotors in the centrifuges. Ralph Langner, "Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve", (2013, November). Retrieved from: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf; Operation Orchard led by the Israeli air force could be seen as an example of a combined preventive strike with kinetic and cyber means.

[22] Kim Zetter, *Countdown to Zero day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Crown Publishing: 2014).

[23] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, (New York: Broadway Paperbacks: 2012).

[24] Ben Buchanan, *The Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System*, (Oxford: Oxford University Press: 2017).

[25] David E. Sanger and Mark Mazetti, "US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict", *The New York Times*, (2016, February 16). Retrieved from: https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html; James Ball, "US Hacked Into Iran's Critical Civilian Infrastructure For Massive Cyberattack, New Film Claims", *BuzzFeed*, (2016, February 16). Retrieved from: https://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma?utm_term=.ile5noYzJy#.kyVJaBdP87.

never used".[26] Defense does not necessarily buy deterrence, nor deterrence defense.[27] Where defense dissuades the adversary by means of presenting an unvanquishable military force, deterrence dissuades by presenting the certainty of a retaliatory devastation.[28]

Few cyber conflict topics have received more attention than cyber deterrence. For the most part, the existing literature uses the term to refer to deterrence of cyberattacks by an adversary, and can be grouped into three buckets. The first group of scholars argue that cyber deterrence does not have distinctive problems and works (or occasionally fails) like conventional deterrence. Dorothy Denning believes that cyberspace strongly resembles traditional domains.[29] According to her, cyber deterrence can therefore be achieved through existing regimes.[30] The second group of scholars believes that cyber deterrence has its unique set of issues, but as long as we further specify the issue area, the problems can largely be solved. Joseph Nye Jr.'s discussion of deterrence is a prominent example.[31] He notes that conventional cyber deterrence is difficult, but we could instead focus on deterrence by economic entanglement and norms to overcome barriers.[32] Lucas Kello argues that cyber deterrence does not work as a strategy, but we could aim for punctuated deterrence instead; we should not deter individual actions but a series of actions.[33] The last group of scholars argues that cyber deterrence does not work and will *never* work. Richard Harknett argues that cyber deterrence is impossible due to the structure of cyberspace.[34] In his view, we need to move away from the deterrence paradigm and consider different forms of strategy, such as persistence.[35] This paper does not address cyber deterrence as defined above; instead, it focuses on the use of a cyber capability to deter a certain type of (military) means of an adversary.

[26] Bernard Brodie, "The Anatomy of Deterrence", *RAND Corporation*, (1958, July 23). Retrieved from: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM2218.pdf.

[27] Art, "To What Ends Military Power", p. 7.

[28] Ibid. Some scholars instead distinguish between deterrence by detail and deterrence by punishment.

[29] The scholars note that "Studies of 'cyber deterrence' raise as many problems as would be raised by a comparable study of 'land deterrence.' Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence", *JFQ*, 77 (2015)8-15. Retrieved from: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf, p. 15.

[30] Ibid.

[31] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security*, 43:3 (Winter, 2016/2017)44-71.

[32] Ibid.

[33] Lucas Kello, *Virtual Weapon and International Order*, (Yale: Yale University Press: 2017); also see: Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence", *Journal of Strategic Studies*, 40:1-2(2017)92-117.

[34] Richard J. Harknett and Joseph S. Nye, "Is Deterrence Possible in Cyberspace?" International Security, 42:2 (2017)196-199; Also see: Brad D. William, Meet the scholar challenging the cyber deterrence paradigm, (July 19, 2017) *The Fifth Domain*. Retrieved from: https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/; Richard J. Harknett and Michael P. Fischerkeller, "Deterrence is Not a Credible Strategy for Cyberspace", Orbis 61:3 (2017)381-393.

[35] Ibid.

OCC tend to be transitory in nature, meaning they only have the "temporary ability to access a computer system or network to cause harm or damage to living and material entities".[36] The transitory nature of a capability is determined by both technical (e.g. type of vulnerability, access and payload used) and non-technical (e.g. the number and type of actors the capability is used against) factors.[37] This feature, combined with their clandestine nature, makes it difficult to prove you have a specific type of capability pre-deployment. Hence, state actors can talk about offensive cyber capabilities whether or not they actually have them; such talk is intended to convey to other actors the impression that the talking nation does have the talked-about capabilities. But since the fact of possession cannot be verified by those other actors nor demonstrated by the talking state, such talk is cheap talk.[38]

Cheap talk, however, is not by definition meaningless and may under certain circumstances still have an impact. One of the key factors which is said to affect the effectiveness of cheap talk is reputation.[39] More specifically, post-hoc revelations about an actor's capability – either intentionally or non-intentionally – can add to the reputation and credibility of the actor's cheap talk on the intention and ability to conduct an offensive cyber operation. This has led to a number of paradoxical dynamics for cyber conflict.

The release of the classified National Security Agency (NSA) documents by Edward Snowden has been described as the most embarrassing episode in the history of the secretive US intelligence agency. It revealed how the NSA maintained a mass-surveillance program over its own citizens, accessed data from companies, intercepted data from global communications networks and stored information of millions of people. Yet, it also exposed the impressive arsenal of the agency. Not least from the Snowden disclosures, *The Washington Post* reported that the US government mounted at least 231 offensive cyber operations in 2011.[40] As Gompert and Libicki note, in

[36] Max Smeets, "A Matter of Time".

[37] OCC exploiting software vulnerabilities are both quantitatively and qualitatively different from conventional weapons in their transitory nature. They are quantitatively different as the introduction of countermeasures - that is, the remediation (patching) of vulnerabilities - occurs on a very rapid and continuing basis. They are also qualitatively different; patching does not only prevent successful exploitation against one system but against any administrator uploading the patch. Even though there are different ways in which patches can be distributed after a software vulnerability is exploited, a defense for one creates a defense for all. Ibid.

[38] Joseph Farrell and Matthew Rabin, "Cheap Talk", *Journal of Economic Perspectives*, 10:3 (1996):103-118; Clayton L. Thyne, "Cheap Signals with Costly Consequences: The Effect of Interstate Relations on Civil War", *Journal of Conflict Resolution*, 50:6 (2006)937-961; Joseph Farrell and Robert Gibbons, "Cheap Talk with Two Audiences", *The American Economic Review*, 79:5 (1989)1214-1223.

[39] Thomas Schelling, *Arms and Influence* (Yale: Yale University Press: 1966), p.124; Alexandra Guisinger and Alastair Smith, "Honest threats: The interaction of reputation and political institutions in international crises", *Journal of Conflict Resolution*, 46: (2002)175-200; Anne Sartori, "The Might of the Pen: A Reputational Theory of Communication in International Disputes", *International Organization*, 56 (2002)121-50.

[40] Barton Gellman and Ellen Nakashima, "US spy agencies mounted 231 offensive cyber-operations in 2011, documents show", *The Washington Post*, (2013, August 30). Retrieved from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

this way, the leaks have ironically "helped it to broadcast how deeply the NSA can supposedly burrow into the systems of others".[41]

Overall, it is more difficult to use OCC as means to deter compared to most other forms of military force. However, it does not mean that it is impossible at all. Especially if an actor is able to show repeatedly what is capable and willing of doing through cyber means it can benefit from this reputation in the future.[42]

C. Compellence

The term compellence in International Relations originates from Thomas Schelling, conceptualizing it as the second form of coercion alongside deterrence.[43] The compellent use of military force serves one of two purposes: i) to stop an activity undertaken by an adversary, or ii) to get an adversary to do something he has not yet undertaken.

The difference between deterrence and compellence hinges upon initiative and timing. The deterrent use of force is based on a promised reaction following an action of the adversary, the timing of which is in principle automatic. The compellent use of force, in turn, is based on a more active strategy of the threatener. For compellence, timing is a critical factor: "too strict a deadline makes compliance impossible, while one too lenient makes compliance unnecessary".[44] Deterrence is usually said to be easier to achieve than compellence; as the deterred party need not to do anything visible, it does not suffer from any reputational damage and can simply argue or imply that it never intended to conduct the activity.

Cyber capabilities have a distinct advantage in this respect. Its effects do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face. More specifically, the compelled actor can deny that the effect was caused by OCC. For example, a three-day disruption of computer systems at an airport leading to massive financial losses and delays could be attributed to a 'general system failure' (a company mistake) whilst in reality it was due to a cyber attack.

This opens up new opportunities for the use of force, although it is dependent on a number of conditions. Not least, the cyber attack needs to cause significant levels of harm or damage to be perceived as a substantial enough cost to change action and delineate the action from the 'constant state' of cyber activity. Whereas plausible deniability is often an advantage to the attacker, in this case the actor should find a

[41] David C. Gompert and Martin Libicki, "Waging Cyber War the American Way" Survival, 57:4 (2015)7-28; also see: Martin Libicki, *Cyberspace in Peace and War*, (Annapolis, Naval Institute Press: 2016), p. 198.

[42] It remains unclear however whether the Snowden revelations helped deterrence or not.

[43] Schelling, *Arms and Influence*, p. 69–91.

[44] Gregory F. Treverton, "Framing Compellent Strategies", *RAND Corporation* (2000). Retrieved from: http://slantchev.ucsd.edu/courses/pdf/treverton-compellence.pdf.

way – either through the design of the weapon or other means – to show that it is conducting this cyber attack in response to the adversary's activity.[45] Finally, in case a compelled actor does not want to reveal it has been attacked, a cyber security firm could instead write a public report exposing the activity.[46] As much of the attribution capability lies with private companies, oftentimes having a strong incentive to publish, this could be a serious concern for states.[47]

OCCs have another distinct advantage when it comes to the compellent use of military force. Unlike kinetic weapons, the attacker can sometimes control the reversibility of the effects of cyber capabilities. Control is based on two dimensions: i) "the adversary's inability to stop or revert the effects of the cyber attack"; and ii) "[the] attacker's ability to stop or revert the effects of the attack at any given time desired".[48] The most detailed account on how reversibility may be achieved is provided by Neil Rowe describing four techniques: i) reversible cryptography, where data is encrypted to prevent use, but can be decrypted after adversary complies; ii) system obfuscation, in which a computer is obfuscated in a reversible manner; iii) data retainment and restoration, where important data is withheld but can be restored; and iv) compromise deception in which adversaries mistakenly think that their system is compromised, but after compliance find out they have been deceived.[49]

The potential reversibility of effect of an OCC may encourage compliance. The adversary may know that, if it backs down, the 'old' situation can be restored. A simple characterization of a conventional situation may be: 'I will keep bombing your critical infrastructure until you stop attacking me'. In this situation, the utility the attacker gains by ceasing the attack is that no further costs (i.e. damage to its critical infrastructure) will be incurred. But the attacker still has to take in its earlier infrastructure losses that were caused during the initial stages of the conflict. In the

[45] See discussion on 'loud cyber weapons', which has primarily been about how to "possibly deter future intrusions". Yet, as this discussion suggests, it should also be considered for the compellent use of force. Chris Bing, "US Cyber Command director: We want 'loud,' offensive cyber tools", *FedScoop*, (2016, August 3). Retrieved from: https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016; Herb Lin, "Developing "Loud" Cyber Weapons", *Lawfare*, (2016, September 1). Retrieved from: https://www.lawfareblog.com/developing-loud-cyber-weapons; Herb Lin, "Still More on Loud Cyber Weapons", *Lawfare*, (2016, October 19). Retrieved from: https://www.lawfareblog.com/still-more-loud-cyber-weapons.

[46] In the case of Stuxnet, for example, the Iranian government has for a long time denied its systems were compromised. Instead, it was researchers from VirusBlokAda, Symantec and the Langner group which initially reported on the sophisticated attacked.

[47] Also see: Max Smeets, "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly*, Forthcoming.

[48] Ibid.

[49] Neil Rowe, "Towards Reversible Cyberattacks", *Proceedings of the 9th European Conference on Information Warfare and Security*, ed. J. Demergis (Reading: Academic Publishing Ltd: 2010), 261-267. Note, however, that reversibility is often a question of time scale. The kinetic destruction of a bridge can be "reversed" by rebuilding the bridge, albeit over a time scale of weeks or months rather than minutes. And in any case, a human death that results from a "reversible" cyberattack on a critical system will not be resurrected when the effects of that cyberattack are reversed. That is, while the direct effects of a cyber capability may be reversible, the consequential effects are almost never reversible. The key issue of reversibility lies in the fact that the reversibility can be implemented by the attacker rather than the defender.

case of a cyber attack, the scenario may be characterized as follows: 'I will corrupt data on 'X' amount of your critical computer systems for every day you keep attacking me'. In this situation, the incentive structure for the attacker has changed; if the actor backs down it will no longer incur costs in the future and retrieves earlier corrupted data.

D. Swaggering

Whereas defense, deterrence and compellence are widely used concepts, 'swaggering' is not part of the common political science vocabulary.[50] As Art indicates:

> "[s]waggering is in part a residual category, the deployment of military power for purposes other than defense, deterrence, or compellence. Force is not aimed directly at dissuading another state from attacking, at repelling attacks, nor at compelling it to do something specific. The objectives for swaggering are more diffuse, ill-defined and problematic than that. Swaggering almost always involves only the peaceful use of force and is expressed usually in one of two ways: displaying one's military might at military exercises and national demonstrations and buying or building the era's most prestigious weapons. The swagger use of force is the most egoistic: it aims to enhance the national pride of a people or to satisfy the personal ambitions of its ruler [...] Swaggering is pursued because of the fundamental yearning of states and statesmen for respect and prestige".[51]

OCC seem to be less valuable for swaggering purposes.[52] Cyber capabilities have a largely non-material ontology, making it difficult to publicly showcase or 'parade' these capabilities. Second, the transitory nature of cyber capabilities is also a problem for swaggering. Cyber capabilities' transitory nature is primarily due to the malleability of cyberspace affecting the life-cycle of a vulnerability and effectiveness of an OCC. The life cycle of vulnerabilities is subject to three delays: i) the awareness delay; ii) the patching delay; and iii) the adaptation delay.[53] The moment actors reveal their capability, it inevitably increases the likelihood of a vendor learning about the vulnerability and assigning a high level of priority to developing a patch (i.e. reducing the awareness and patching delay).[54] Overall, as a document from the East West Institute concludes:

[50] The concept has been used once before in relation to cyber attacks by Neuman and Poznansky. They however misapplied the concept as swaggering is not a form of coercion. Craig Neuman and Michael Poznansky, "Swaggering in Cyberspace: Busting the conventional wisdom and cyber coercion", *War on the Rocks*, (2016, June 28). Retrieved from: https://warontherocks.com/2016/06/swaggering-in-cyberspace-busting-the-conventional-wisdom-on-cyber-coercion/.

[51] Art, "To What Ends Military Power", p. 10-11.

[52] However, this does not mean that a cyber *command or program* cannot be established for prestige purposes.

[53] Smeets, "A Matter of Time".

[54] Ibid.

> “[m]ilitary forces will have distinct interests in keeping cyber weapons secret. [...] Those nations that are developing the most advanced weapons have a strong interest in being able to protect the intelligence surrounding such capabilities”.[55]

4. CONCLUSION

Considering the growing interest in the use of offensive cyber capabilities as a tool for the state, this study assessed to what degree these capabilities have the potential to change the role of military power. We have shown that OCCs have the potential to significantly affect how states use their military power in several ways. First, OCCs have downgraded the role of *deterrence*, except for those states with a credible reputation for being able and willing to conduct offensive cyber operations. However, we indicated that *compellence* is no longer ruled out as a function of military power considering several features of cyber capabilities. Unlike conventional capabilities, the effects of offensive cyber capabilities do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face. The potential to control the reversibility of effect of a cyber capability by the attacker may also encourage compliance. As OCCs can be used as both a preemptive and a preventive strike option, it reemphasizes the potential to use of force for *defensive* purposes. Finally, due to its largely non-material ontology and transitory nature, its symbolic value as a prestige weapon to enhance swaggering remains unclear.

Major powers reap benefits from their nuclear arsenal without using them physically and risk high costs when they are used. This in turn incentivizes the avoidance of warlike behavior and exploitation of peaceful use. Yet, this logic breaks down for cyber capabilities: the benefits from non-use are lower given the limits of deterrence and swaggering; the costs of non-use are higher due to the transitory nature of these capabilities; and the risks of using cyber capabilities are lower. Overall, it means less powerful incentives exist for restraint.

As we have only provided a primer on the topic, there are several avenues for future research. This paper was consciously limited to only assess the role of OCCs with regard to state power. Given that OCCs are normally part of a broader arsenal of capabilities, it is important to discuss the military use of OCC in relation to military capabilities. Further research may therefore conduct a comparative analysis of other assets (nuclear weapons, drones, covert actions) to gain a more holistic understanding of the military contribution of each capability. Also, it has been noted that the growth of the private sector market for OCC leads to new opportunities for states to acquire,

[55] EastWest Institute, “Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace”, (2011). Retrieved from: https://www.eastwest.ngo/sites/default/files/ideas-files/US-Russia%20(1).pdf.

deploy and use these capabilities. It remains unclear, however, to what degree this trend also changes the way in which OCCs can be strategically used by states as a function of military power.

REFERENCES

Alexander, Keith, US Senate, Committee on Armed Services, (2014, April). Retrieved from: http://www.eweek.com/security/nsa-director-says-cyber-command-not-trying-to-militarize-cyberspace.

Anonymous, "Magnitude 4.3 – NORTH KOREA", USGS, (2006, October 9). Retrieved from: https://web.archive.org/web/20140427050803/http://earthquake.usgs.gov/earthquakes/eqinthenews/2006/ustqab/.

Ardant du Picq, Charles, *Battle Studies: Ancient and Modern Battle*, trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

Art, Robert J., "To What Ends Military Power?", *International Security*, 4:4 (1980)3-35.

Ball, James, "US Hacked into Iran's Critical Civilian Infrastructure for Massive Cyberattack, New Film Claims", *BuzzFeed*, (2016, February 16). Retrieved from: https://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma?utm_term=.ile5noYzJy#.kyVJaBdP87.

Bellovin, Steven M., Susan Landau and Herbert S. Lin, "Limiting the undesired impact of cyber weapons: technical requirements and policy implications", *Journal of Cybersecurity*, 3:1 (2017)59–68.

Bing, Chris, "US Cyber Command director: We want 'loud,' offensive cyber tools", *FedScoop*, (2016, August 3). Retrieved from: https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016.

Brodie, Bernard, "The Anatomy of Deterrence", RAND Corporation, (1958, July 23). Retrieved from: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM2218.pdf.

Buchanan, Ben, *The Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System*, (Oxford: Oxford University Press: 2017).

Carter, Ashton, "A Lasting Defeat: The Campaign to Destroy ISIS", Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, (October 2017). Retrieved from: https://www.belfercenter.org/LastingDefeat.

Collier, Jamie, "State Proxies & Plausible Deniability: Challenging Conventional Wisdom", *Cybersecurity Intelligence*, (2015, September 24). Retrieved from: https://www.cybersecurityintelligence.com/blog/state-proxies-and-plausible-deniability-challenging-conventional-wisdom-644.html.

Dao, Jim, Giang The Huong Tran and Tu Ngoc Trinh, "New Law on Cyber Security in Vietnam", *Tilleke & Gibbins* (2016, June 3). Retrieved from: http://www.tilleke.com/resources/new-law-cyber-security-vietnam.

Denning, Dorothy E., "Rethinking the Cyber Domain and Deterrence", *JFQ*, 77 (2015)8-15. Retrieved from: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf.

E-ISAC, SANS ICS, "Analysis of the Cyber Attack on the Ukrainian Power Grid" (2016, March 18). Retrieved from: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

EastWest Institute, "Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace", (2011). Retrieved from: https://www.eastwest.ngo/sites/default/files/ideas-files/US-Russia%20(1).pdf.

Farrell, Joseph, and Matthew Rabin, “Cheap Talk”, *Journal of Economic Perspectives*, 10:3 (1996):103-118.

Farrell, Joseph, and Robert Gibbons, “Cheap Talk with Two Audiences”, *The American Economic Review*, 79:5 (1989)1214-1223.

FireEye, “Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks”, *WhitePaper*, (2012). Retrieved from: http://www.softbox.co.uk/pub/ reeye- advanced-targeted-attacks.pdf.

Frendesen, Christoffer, “Colombia sends officials to Estonia for cyber defense training”, *Columbia Reports*, (2014, September 2). Retrieved from: http://colombiareports.com/colombias-govt-sends-security-forces-estonia-cyber-defense-training/.

Gellman, Barton, and Ellen Nakashima, “US spy agencies mounted 231 offensive cyber-operations in 2011, documents show”, *The Washington Post*, (2013, August 30). Retrieved from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

Gerden, Eugene, “Russia to spend $250m strengthening cyber-offensive capabilities”, *SC Magazine UK*, (2016, February 4). Retrieved from: http://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive- capabilities/article/470733.

Gompert, David C., and Martin Libicki, “Waging Cyber War the American Way”, *Survival*, 57:4 (2015)7-28.

Guisinger, Alexandra, and Alastair Smith, “Honest threats: The interaction of reputation and political institutions in international crises”, *Journal of Conflict Resolution*, 46: (2002)175-200.

Harknett, Richard J., and Joseph S. Nye, “Is Deterrence Possible in Cyberspace?” *International Security*, 42:2 (2017)196-199.

Harknett, Richard J., and Michael P. Fischerkeller, “Deterrence is Not a Credible Strategy for Cyberspace”, *Orbis* 61:3 (2017)381-393.

Hayden, Michael, *Playing the Edge: American Intelligence in the Age of Terror*, (New York: Penguin Press: 2014).

Herr, Trey, “PrEP: A Framework for Malware & Cyber Weapons”, *The Journal of Information Warfare*, 13:1(2014).

Israel Defense, “Turkey Launched Cyber Warfare Command”, (2014, April 13). Retrieved from: http://www.israeldefense.co.il/en/content/turkey-launched-cyber-warfare-command.

Kaspersky Lab’s Global Research & Analysis Team, “BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents”, Securelist, (2016, January 28). Retrieved from: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/.

Kello, Lucas, *Virtual Weapon and International Order*, (Yale: Yale University Press: 2017).

Langner, Ralph, “Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve”, (2013, November). Retrieved from: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Libicki, Martin, *Cyberspace in Peace and War*, (Annapolis, Naval Institute Press: 2016).

Lin, Herbert, “Developing ‘Loud’ Cyber Weapons”, *Lawfare*, (2016, September 1). Retrieved from: https://www.lawfareblog.com/developing-loud-cyber-weapons.

Lin, Herbert, “Still More on Loud Cyber Weapons”, *Lawfare*, (2016, October 19). Retrieved from: https://www.lawfareblog.com/still-more-loud-cyber-weapons.

Lindsay, Jon, “Stuxnet and the Limits of Cyber Warfare”, *Security Studies*, 22:3 (2013)365-404.

Lyngaas, Sean, “Pentagon Chief: 2017 budget includes $7B for cyber”, *FCW* (February 2, 2016). Retrieved from: https://fcw.com/articles/2016/02/02/dod-budget-cyber.aspx.

Mathew, S., R. Giomundo, S. Upadyaya, M. Sudit and A. Stotz, “Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams”, *VizSEC ‘06, Proceedings of the 3rd International Workshop on Visualization for Computer Security* (2016)1-6.

McGuffin, Chris, and Paul Mitchell, “On domains: Cyber and the practice of warfare”, *International Journal*, 69:3 (2014):394-412.

Michael, Melissa, “NotPetya and Wannacry: Have we seen the last?” *F-Secure* (2017, July 7). Retrieved from: https://business.f-secure.com/notpetya-and-wannacry-have-we-seen-the-last.

NATO CCD COE, “NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit”, (2016, July 21). Retrieved from: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

Neuman, Craig, and Michael Poznansky, “Swaggering in Cyberspace: Busting the conventional wisdom and cyber coercion”, *War on the Rocks*, (2016, June 28). Retrieved from: https://warontherocks.com/2016/06/swaggering-in-cyberspace-busting-the-conventional-wisdom-on-cyber-coercion/.

Nye, Joseph S., “Deterrence and Dissuasion in Cyberspace”, *International Security*, 43:3 (Winter, 2016/2017)44-71.

Peterson, Dale, “Offensive Cyber Weapons: Construction, Development and Employment”, *Journal of Strategic Studies*, (2013)36:1.

Raghuvanshi, Vivek, “New Indian Cyber Command Urged Following Recent Attacks”, *Defense News*, (2016, June 6). Retrieved from: https://www.defensenews.com/2016/06/06/new-indian-cyber-command-urged-following-recent-attacks/.

Rid, Thomas, and Ben Buchanan, “Attributing Cyber Attacks”, *Journal of Strategic Studies*, 38:1-2 (2015)4-37.

Rid, Thomas, and Peter McBurney, “Cyberweapons”, *The RUSI Journal*, 157:1 (2012):6-13.

Rowe, Neil, “Towards Reversible Cyberattacks”, *Proceedings of the 9th European Conference on Information Warfare and Security*, ed. J. Demergis (Reading: Academic Publishing Ltd: 2010), 261-267.

Sanger, David E., and Mark Mazetti, “US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict”, *The New York Times*, (2016, February 16). Retrieved from: https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Sanger, David E., David D. Kirkpatrick and Nicole Perlroth, “The World Once Laughed at North Korean Cyberpower. No More”, *The New York Times* (October 15, 2017). Retrieved from: https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

Sanger, David, Confront and Conceal: *Obama’s Secret Wars and Surprising Use of American Power*, (New York: Broadway Paperbacks: 2012).

Sartori, Anne, “The Might of the Pen: A Reputational Theory of Communication in International Disputes”, *International Organization*, 56 (2002)121-50.

Sauer, Tom, “The Preventive and Pre-Emptive Use of Force: To be Legitimized or to be De-Legitimized?”, *The Hoover Institution*. Retrieved from: http://www.ethical-perspectives.be/viewpic.php?TABLE=EP&ID=493.

Schelling, Thomas, *Arms and Influence*, (Yale: Yale University Press: 1966).

Secretariat of the Security Committee, “Finland’s Cyber Security Strategy”, (2013). Retrieved from: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

Sharafedin, Bozorgmehr, “Iran to expand military spending, develop missiles”, *Reuters*, (2017, January 9). Retrieved from: https://www.reuters.com/article/us-iran-military-plan/iran-to-expand-military-spending-develop-missiles-idUSKBN14T15L.

Shires, James, and Max Smeets, “The Word Cyber Now Means Everything—and Nothing at All”, *Slate*, (2017, December 1). Retrieved from: http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_lost_all_meaning.html.

Smeets, Max, “A matter of time: On the transitory nature of cyberweapons”, *Journal of Strategic Studies*, (2017)1-28.

Smeets, Max, “Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks”, *9th International Conference on Cyber Conflict*, (Tallinn: NATO CCD COE Publications: 2017).

Smeets, Max, “US Cyber Command: An Assiduous Actor, Not a Warmongering Bully”, *The Cipher Brief*, (March 4, 2018). Retrieved from: https://www.thecipherbrief.com/us-cyber-command-assiduous-actor-not-warmongering-bully.

Thomas, Bindiya, “UAE Military to Set Up Cyber Command”, (2014, September 30), *DefenseWorld*. Retrieved from: http://www.defenseworld.net/news/11185/. UAE_Military_To_Set_Up_Cyber_Command#.WW4nJYjyiUk.

Thyne, Clayon L., “Cheap Signals with Costly Consequences: The Effect of Interstate Relations on Civil War”, *Journal of Conflict Resolution*, 50:6 (2006)937-961.

Tor, Uri, “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence”, *Journal of Strategic Studies*, 40:1-2(2017)92-117.

Treverton, Gregory F., “Framing Compellent Strategies”, *RAND Corporation* (2000). Retrieved from: http://slantchev.ucsd.edu/courses/pdf/treverton-compellence.pdf.

Weaver, Nicholas, and Dan Ellis, “Reflections on Witty: Analyzing the Attacker”, *Security*, 29:3 (2004) 34-37.

Werkhäuser, Nina, “German army launches new cyber command”, *DW*, (April 1, 2017). Retrieved from:http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517.

William, Brad D., “Meet the scholar challenging the cyber deterrence paradigm”, (July 19, 2017) *The Fifth Domain*. Retrieved from: https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

Zetter, Kim, “Everything We Know About Ukraine’s Power Plant Hack”, *Wired*, (20 January 2016). Retrieved from: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

Zetter, Kim, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, *Wired*, (3 March 2016). Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zetter, Kim, *Countdown to Zero day: Stuxnet and the Launch of the World’s First Digital Weapon*, (New York: Crown Publishing: 2014).