Developing a Proportionate Response to a Cyber Attack

Jarno Limnéll

Aalto University
SCIENCE + TECHNOLOGY
WORKING PAPERS

Aalto University publication series
SCIENCE + **TECHNOLOGY** 3/2016

Developing a Proportionate Response to a Cyber Attack

Jarno Limnéll

Aalto University
School of Electrical Engineering
Communications and Networking

Professor Jarno Limnéll
jarno.limnell@aalto.fi
PO Box 13000
FI-00076 AALTO
Finland

Aalto University publication series
SCIENCE + **TECHNOLOGY** 3/2016

ISBN 978-952-60-6720-9 (pdf)
ISSN-L 1799-4896
ISSN 1799-4896 (printed)
ISSN 1799-490X (pdf)
http://urn.fi/URN:ISBN:978-952-60-6720-9

Unigrafia Oy
Helsinki
2016

Finland

Acknowledgements

The debate on both the impacts of cyber attacks and how to response to attacks is active but precedents are only a few. Strategies and political speeches are always (at least partially) declaratory and vague by nature, and beyond these declarations the practical reality of cyber security as a matter of national security issue is challenging. At the same time cyber issues have catapulted into the highest of the high politics, cyberpolitics, and the line of digital and physical is blurring in many ways. Also defensive, intelligence or offensive cyber capabilities are difficult to assess, because governments are holding their abilities very secret, and cyber capabilities cannot be calculated in the same way as tanks or fighter planes. Primary intention of this paper is to encourage the national policies concerning on the issue of how cyber attacks should be treated and lead to policies for response. The paper determinates five variables which policymakers need to consider when evaluating appropriate response to a state-sponsored cyber attack. As offensive cyber activity becomes more prevalent, policymakers will be challenged to develop proportionate responses to disruptive or destructive attacks. Already, there has been significant pressure to "do something" in light of the allegedly state-sponsored attacks. Past experience suggests that most policy responses have been made ad hoc. But proportionate response is a complicated political question and also situational dependent. This paper analyses in a comprehensive way how cyber attacks will be treated especially as a political question, and this paper represents a rough example of the framework that policymakers should build on. Combining incident impact and policy options it outlines the different levers of cyberpolitics that can be applied in response to escalating levels of cyber incident. The cyber response framework of the state is also an integral part of state´s cyber deterrence.

Espoo, 17 March 2016
Jarno Limnéll

Contents

1. Cyberpolitics in today´s world

Cybersecurity has become a focal point for conflicting domestic and international interests, and increasingly for the projection of state power. When we are living the dawn of the cyber era it is necessary to realize what is often forgotten or neglected is the increasing importance of cyberspace as a political domain. When evaluating the cyberspace from the nation-state´s point of view, today´s topical questions are very political, and primarily cyber domain should be treated as a political domain. And when politics is involved, the questions of power are always present. For example referring to war, the cyber instrument is, like land, sea and air power, a means to achieve a political aim. The strategic use of cyberspace to pursue political goals and seek geostrategic advantage is rapidly increasing in today´s world.

Until recently, cyber domain was considered largely a matter of low politics, background conditions and processes. Lately events connected to cyberspace like Sony Hack, Duqu 2.0, economic cyber espionage accusations between China and the United States and the role of cyber in Ukraine war have catapulted cybersecurity into the highest of the high politics, *Cyberpolitics*[1]. With the creation of cyberspace, a new arena for the conduct of politics is taking shape, and we may well be witnessing a new form of politics. The process of "cyberization[2]" which refers to the ongoing penetration of all political fields by different mediums of cyber domain, there is also a significant lack of discussion and debate with scholars and experts how politically cyber-attacks should be treated. The ubiquity, fluidity, and anonymity of cyberspace have already challenged such concepts as leverage and influence, national security and diplomacy, and borders and boundaries in the traditionally state-centric arena of international relations. It is vital to understand cyber less as a technological issue, but as a strategic challenge.

The concept of cyberpolitics is useful. The term refers to the conjunction of two processes: those pertaining to politics surrounding the determination of who gets what, when and how, and those enabled by the uses of cyberspace, a new arena of digital interactions. All politics, in the cyber and physical arenas, involves conflict, negotiation and bargaining over the mechanisms, institutional or otherwise, to resolve in authoritative ways the contentions over the nature of

[1] Choucri, "Cyberpolitics in International Relations", 267–271.
[2] Kremer and Müller, Cyberspace and International Relations, xi.

particular sets of core values. Cyberpolitics is being created in both national and international levels, but both the cyberpolitics and cyber domain has created new conditions which have does not have clear precedents even if cyber issues are the core issues in nation-states' foreign and security policy. In coming years we will see through actual cases what the content of cyberpolitics will really be like.

The recent development illustrates the extent to which the cyber domain has gradually and inexorably become central to most facets of human existence. At the same time the concepts of attack, defence, deterrence, international cooperation and espionage take on new meanings. We do not yet have a clear understanding on these changes in political decision-making arenas. There are many power-related strategic questions on the table, but still too few answers and too little real political desire to find the answers. The following five topical and intertwined cyber power related trends are vital to keep in mind while creating political framework to response state-sponsored cyber attacks:

- The general trend of digitalization and the emphasis on the importance of the cyber domain have made states more aggressive. Because various operations in the cyber domain are felt to be "softer" use of power than use of physical force, states' threshold for using cyber capabilities is rather low.
- There is ongoing cyber arms race in the world. More than 100 of the world's militaries have some sort of organization in place for cyberwarfare and over 40 countries worldwide have published their National Cyber Strategy.[3] The world is moving toward a greater strategic use of cyber capabilities to persuade adversaries to change their behavior.
- The difference between peace and war has become considerably more opaque. Future conflicts are probably more vague, lacking a clear beginning or end, and in between things "just happen." In cyber domain, the distinction between combatants and civilians or legal and illegal activities are harder to draw.
- International cooperation in cyber matters is still regrettably weak. Political collaboration is an absolute prerequisite for developing security, but rather than strengthening it states have turned inward. At the moment, a pretty strong distrust exists between states. Power and capabilities remain unevenly distributed within the cyber domain, although a growing number of states are enhancing their influence through the acquisition of cyber capabilities.
- Nation-states are already testing the boundaries of the cyber battlefield and cyber domain has forced them to rethink their security and military concepts. The need for establishing boundaries via cyberpolitics is critical.

All these five issues emphasize the importance of creating a political framework: How to confront and response a cyber attack which consists of deliberate hostile action taken in cyberspace for a political or national security purpose. An

[3] Singer and Cole, "The Reality of Cyberwar."

equally important question is how to include the breadth of national cyber security issues and functions in times of both peace and war, and across the different both cyber and physical components of national power,[4] e.g. to exert cyber power. The "cyber playbook" is pretty empty and at the same time the world is moving towards greater strategic use of cyber-weapons to persuade adversaries to change their behavior, and cyber will be an element of all crises and wars we're seeing and going to see in the future. Both international and national discussion about cyberattacks and how to respond to them is overdue even if the strategic importance of digital domain is widely acknowledged.

[4] Hathaway and Klimburg, "Preliminary Considerations," 27-29.

2. Cyberattacks, what are they?

It is challenging is to understand how digital domain is blurring our dichotomies – how we as humans are tend to organize the world. If there's no war, peace prevails. If you don't need to worry about insecurity, you feel safe. If you didn't initially attack, you're acting in self-defense, and "you're either with us or against us." Cyberspace—and cyberwarfare taking place in it—blurs many of the conventional borders used for making such distinctions and understanding war as solely physical consequences is an unnecessarily limited view. At the moment there are no clear understand what cyberwarfare or even different cyber activities include and what not, and that is the reason why so many cyber incidents are labelled as cyberwar. This makes the creation of cyberpolitics even more challenging.

We need first to understand what an attack is – espionage, kinetic equivalent, informational – since that affects to the considerations of proper response. The Tallinn Manual's Rule 30 offers the definition of "cyber attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[5] But, as mentioned also in Tallinn Manual, cyber attacks seldom involve the release of direct physical force against the targeted cyber system; yet, they can result in great harm to individuals or objects.[6] In this paper cyber attack, as a concept, is understood very widely in national and political context: *A cyber attack consists of any deliberate hostile action taken in cyberspace for a political or national security purpose.*

Experts have speculated about the potential consequences of different kind of cyber attacks. Scenarios range from DDoS-attacks to a virus that scrambles financial records or incapacitates the stock market and to a false message that causes a nuclear reactor to shut off or a dam to open. When analyzing the impacts of cyber attacks from cyberpolitics point of view, it is vital to understand the blurred relationship between the cyber domain and the physical world. We can classify roughly four fields of activities of the cyber and the physical worlds: Physical-physical, physical-cyber, cyber-cyber and cyber-physical.[7] The placing

[5] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, 106-110.
[6] Ibid.
[7] Lehto, Neittaanmäki, Cyber Security: Analytics, Technology and Automation, Springer, 34-35.

an activity to one of the fields of the fourfold table depends on the world where the activity is executed and occurs. The fourfold table supports especially the modelling of activities of the overlapping parts of the cyber and the physical worlds and helps top understand how cyber and physical world activities are interconnected which is important when considering reasonable response. The fourfold table can also be used for assuring that both the cyber and the physical world aspects are concerned. This is important since often cyber is thought only as incidents occurring in digital domain without physical impacts. Recently the interest in the kinetic cyber has increased. Kinetic cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes. But most cyber attacks will not produce destructive effects similar to kinetic weapons, but will instead seek to disrupt data and services, create confusion, damage networks and computers, including software and computers embedded in weapons systems. It must be a requirement that the seriousness of the effects occurring in cyber, caused either via cyber or physical, is understood in response analysis. The latest study reveals that majority of IT professionals in rate a serious cyberattack affecting critical services and causing loss of life as highly likely within the next three years.[8]

[8] Aspen Institute and Intel Security, Critical Infrastructure Readiness report, Holding the Line Against Cyberthreats.

3. Five variables

At the moment governments are unprepared to properly respond state-sponsored cyber attacks. When the strategic importance of cyber domain increases and offensive cyber activity becomes more prevalent, policymakers are challenged to develop cyberpolitics for proportionate responses to disruptive or destructive attacks. There are not clear and established "playbooks" how to response a cyber attack especially if the attacker is most likely considered as a state. Policy makers are still wrestling with the complicated questions of how best to respond to cyber attacks. But finding a timely, proportionate, legal, and discriminatory response is complicated by the difficulty in assessing the damage to national interests and the frequent use of proxies. Finding a timely, proportionate, legal, and discriminatory response – and let others to know it – is essential in the context of cyber power. When the strategic importance of cyber domain increases and offensive cyber activity becomes more prevalent, policymakers are challenged to develop cyberpolitics for proportionate responses to disruptive or destructive attacks.

When does a cyber attack (or threat of cyber attack) give rise to a right of self-defense, including armed self -defense, and when should it? In determining the appropriate response to a state-sponsored cyber attack, policy makers need to consider (at least) the following five variables[9].

First, attributing cyber attacks to their sponsor remains a significant challenge. The attribution problem has technical and human components, and both are challenging. Attribution problem will only become more critical as we move into a new era of cyber conflict with even more attacks ignored, encouraged, supported, or conducted by national governments.[10] Attacking or going after malcontents are not simple and it's difficult to discern the difference between a military, nation-state, or non-state attack. Cyberspace allows for a great deal of anonymity and attacks can be routed through servers all over the globe to mask its origin. In politics, under pressure, responses are likely to be made quickly with incomplete evidence and attract a high degree of public skepticism. This creates risks for policymakers. Misattributing a cyber incident could cause a response to be directed at the wrong target. When considering proportionate re-

[9] Compare Feakin, "How to Respond to a State-Sponsored Cyber Attack."
[10] Healey, Beyond Attribution: Seeking National Responsibility for Cyber Attacks.

sponse policymakers should understand the level of confidence they have in attributing the attack. The degree of attributional certainty will have a direct impact on the action taken. One key issue is also information sharing partner nations, which is important to identify where an attack came from, what it affected and what might be next. The ability to attribute an attack to a specific source is important for maintaining credibility and ensuring legitimacy at home and abroad.

Second, in cyberpolitics policymakers should assess the cyber attack´s effects. The challenge with calculating proportionality in the cyber context resides in the speed and covert nature of cyber attacks: it is difficult to readily establish their magnitude and consequences. Required information can also be hard to get, since for example financial institutions and companies might be reluctant to provide information on the damage suffered because of business confidentiality.[11] Assessing the whole damage caused by a cyber attack is difficult. It can take weeks, if not months, for computer forensic experts to accurately and conclusively ascertain the extent of the damage done to an organization's computer networks. For example, it took roughly two weeks for Saudi authorities to understand the extent of the damage of the Shamoon incident, which erased data on thirty thousand of Saudi Aramco's computers.[12] In many cases states and companies find out that they have been hacked months (or even years) after it happened.

Third, policymakers must take into the consideration the current national security and cyber security strategies which (usually) declare the general policy guidelines of the state concerning on the political willingness to leverage cyber power. If a state is part of international alliances and organizations, their policy guidelines must also be taken in to consideration when thinking proportionate response. Otherwise a state can be accused for not following the agreed and shared policy.

Fourth, it is also a question of the options which a state is able to use. It is said that every nation-state can respond using at least four instruments: Diplomatic, informational, military and economic.[13] Responses need not to be limited to cyberspace, since nothing bars a state from using other channels, though each carries its own risks. The key issue is to consider which cyber or physical (or other) counter measures can be used (as part of nation-state´s "response arsenal") and which measures should be used in each case. This is a question of the levers of national power at a state's disposal and willingness to use them.

Fifth, there's also a possibility that when a cyber attack occurs, the nation-state may overreact. Several cyber experts have estimated that the overreaction

[11] Roscini, Cyber Operations and the Use of Force in International Law.
[12] Bronk and Tikk-Ringas, The Cyber Attack on Saudi Aramco.
[13] E.g. Thomas, Creating Cyber Strategists: Escaping the "DIME" Mnemonic.

is very real.[14] Cybersecurity professionals can also have an incentive to trumpet the threat of cyber attack that at times may heighten the risk of overreaction. Even if there is probably a great political pressure after occurred cyber attack, political prudence is needed. At least in certain level restraint should be encouraged, and the importance of it is needed. Self-restraint is a concept that is relevant to keep in mind to de-escalation of the activities, especially if kinetic response is considered. In general, deterring escalation requires that the adversary believe that escalation will result in a worse outcome than restraint, which can be occasionally a stronger way to manifest national cyber power.

[14] E.g. McGraw and Fick, Separating threat from the hype: What Washington needs to know about cyber security.

4. OPM hack case – an example

A good example of the need to answer all five variables is the cyber attacks against the United States Office of Personnel Management (OPM) in 2015.

The key question after attacks was how the U.S. would respond to the attacks, for which it seemed likely to hold China responsible (although not formally)? The Chinese government denied its involvement, and has said that the U.S. is just using the China threat to justify expanding cyber capabilities.[15] In the end of 2015 China said that OPM hack was a criminal act perpetrated by hackers, and not a state-sanctioned cyber attack. The certainty of attribution has stayed vague, at least in public. Also the messages from the U.S. officials have been contradictory. Even if the U.S. government has took a strong stance to blame China, the NSA´s director publicly said that "it's merely an assumption that the Chinese government was behind the hack."[16] What about the consequences? Even today it is unclear what the real impacts of the attacks were. It has publicly told that the hacks of the OPM databases compromised 22.1 million people,[17] but is it unclear what the indirect implications will be in a longer period (how the information will be utilized).

Few months before the attacks the U.S. Defense Secretary Ash Carter announced[18] an updated cyber strategy[19], according to which the United States would retaliate against major cyber attacks, either with cyber tools or by other means. US response has also been discussed with allies, and several different options for response have been presented. The OPM cyber attack was the first test case of the US cyber strategy, and it seemed to fail. The challenge has been the balance between strategy and real actions. There have been also a lot of political discussions in the U.S. that in which way these attacks should be even called. Some have called the OPM hack as an act of war,[20] and some have said that it is just normal espionage what all countries are doing.

Defense Secretary Ash Carter and National Security Agency Director Michael Rogers have announced several times that U.S. policy makers need to decide

[15] Ministry of Foreign Affairs of the People´s Republic of China, "Foreign Ministry Spokesperson Lu Kang's Regular Press Conference on June 15, 2015."
[16] Tucker, "NSA Chief : Don´t Assume China Hacked OPM".
[17] Nakashima, "Hacks of the OPM."
[18] Stewart, "Pentagon's New Cyber Strategy Cites U.S. Ability to Retaliate."
[19] The DOD Cyber Strategy, 11, 25.
[20] Paletta, "When Does a Hack Become an Act of War?"

how they are going to respond to cyberattacks as countries become more brazen in their attempts. So what have been the options in OPM case for the U.S. to response? There have been on the table (in public discussions) at least seven policy options,[21] that are relevant for retaliating and deterring these kind of cyber attacks by foreign nation-states, including their risk of escalation: 1) Passive deterrence: Doing nothing directly towards China. 2) Diplomatic Protests: A largely symbolic response with hardly any risk of escalation. 3) Legal Measures: Legal action against Chinese organizations and individuals. 4) Economic sanctions: Important in the Chinese case is that the U.S. economy is heavily dependent on interaction with China. 5) Retaliation in cyberspace: By retaliating the U.S. would show that future cyber intrusions of this scale will not be tolerated. 6) Military retaliation: Such action would probably trigger a military response back from China and could culminate in a dangerous process of escalation. 7) Covert retaliation in cyberspace: It is the invisibility, and therefore unpredictability, of covert retaliation that might deter China – if it was the attacker of the OPM in the first place.

The OPM case shows well the variables which are involved when politically considering how to respond cyber attacks. The fact that even the United States, the leading major cyber power, finds it hard to respond to a major breach of its cyber security shows that less powerful states will have even more problems in retaliating against cyber attacks. At the same time a study[22] found that 92 percent of Americans believe the U.S. government should react in some way to cyberattacks if government data is compromised. High-profile cyber attacks by nation-states are a relatively new phenomenon, in which there isn't a roadmap of deterrents and responses.

[21] Van der Meer and Van der Putten. US Deterrence against Chinese Cyber Espionage.
[22] Vormetric. Media Advisory, 1.

5. Political response model

U.S. National Security Agency chief Michael Rogers has said that "Because an opponent comes at us in the cyber domain doesn't mean we have to respond in the cyber domain."[23] The statement describes well the blurring reality of kinetic and non-kinetic response to cyber attacks. There is no reason to believe that a cyber attack of any form requires a directly proportionate cyber response. Given the reality of asymmetric cyber reliance, the implication that response to a cyber attack should not be confined to a cyber response.

Responses can be classified into two categories, kinetic and non-kinetic and are dictated by the nature and character of the attack. It is also possible to response in both kinetic and non-kinetic means. Even if the line of using kinetic and/or non-kinetic ways to response, it is usually argued that kinetic responses should remain only allowable if the attack has intended lethal effects, causes human suffering or loss of life, or human rights are directly violated.[24] This is too narrow approach. Digitally dependent societies can be in a big trouble for example if attacker confuses the financial records of the state or steals a great amount of intellectual property – no one dies but consequences can be very severe to state´s security and competitiveness. However, it becomes difficult to justify military response to a cyber attack that does not cause kinetic or physical harm as in a conventional or Clausewitzian sense.[25] Further, in cyberspace, it may be difficult to distinguish an attack from espionage or vandalism, neither of which historically is enough to trigger a proportionate response.

Figure 1 represents a one rough example of the framework that policymakers should build on. Combining incident impact, policy options, risks, and proportionality, it outlines the different levers of cyberpolitics that can be applied in response to escalating levels of cyber incident. The purpose of the framework is to illustrate at the same time both the impact and the possible response options which should be analyzed much more carefully within the policymakers when a state is creating their own cyber re response model. The framework plots the

[23] Hackett, "Let´s Get Physical? United States Weighs Options When It Comes to Cyber Attack".
[24] E.g. Wester, "Just Cyberwar".
[25] Lin, P., Fritzsch L. and Rowe, N, "Is It Possible to Wage a Just Cyberwar?"

effects of a cyber incident, with website defacement at one end of the scale and loss of life at the opposite end.[26] This is described against the level of response, ranging from media statements to military responses. Across the response spectrum there will be inherent political and legal risks associated with each decision, and risks increase as the level of the response increases.[27]

As Tobias Feakin[28] argues, policymakers should clearly understand also the costs associated with each response. Each response will have an impact on a country´s diplomatic relations, reputation, and military and intelligence operations. Effects need to be understood before a response is chosen as well as the four variables which were explained earlier in this paper. It is also questionable in cyberspace how far "active defense" or the concept of "hacking back" should go. This is a topical question especially in private sector (which is often the main target of state-sponsored cyber attacks) where "active defense" has gained gained currency as frustration grows about the inability of the government to stem lawlessness in cyberspace.[29] If private companies are too active and decisive in their hacking back operations, they may mix the state´s response model significantly. It should be noted that international law categorically prohibits a non-state actor (in this case a corporation) from actively engaging a hostile state, even if victimized by a cyber attack.[30] Best course of action for a corporation is to contact their own government to possible respond on their behalf. This requires a strong partnership between the government and the private sector.

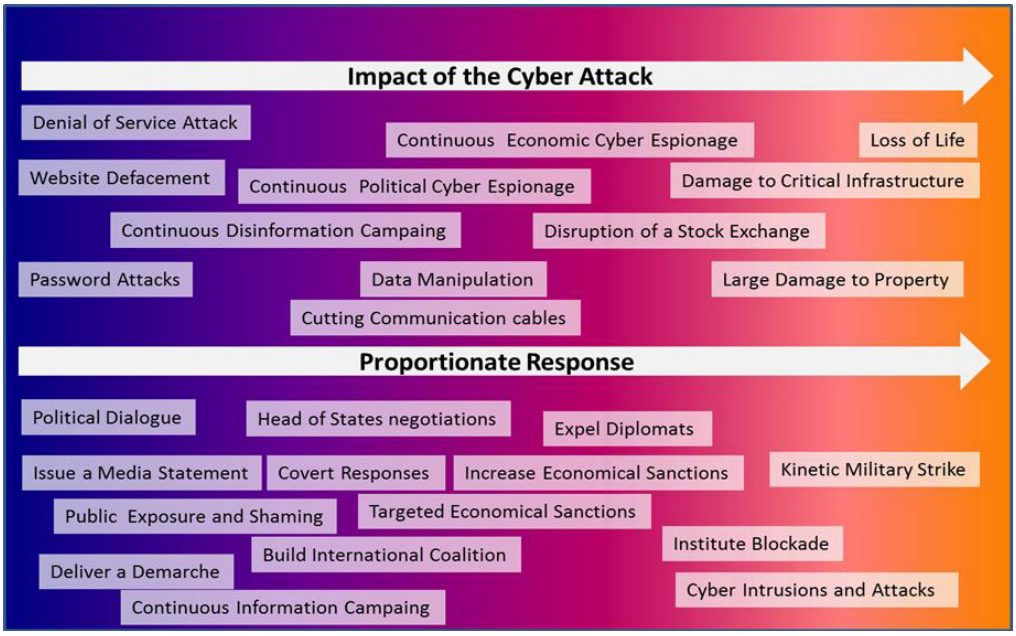

Figure 1. The framework of the impacts of cyber attacks and proportionate responses.

[26] See Feakin, "How to Respond to a State-Sponsored Cyber Attack".
[27] Williams, "The Joint Force Commander´s Guide to Cyberspace Operations".
[28] Feakin.
[29] Timberg, Nakashima, Douglas-Gabriel, "Cyberattacks Trigger Talk of Hacking Back."
[30] Garrie. "Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors".

6. Conclusion

The role of the cyber domain is increasingly shaping the global security environment and the power dynamic between states and other actors. At the same time cyber capabilities are reaching towards a more advanced level. We have entered an unstable and suspicious era, and we are doing so without a clear roadmap of tested political fundamentals. Strategic and political understanding is needed when creating a response model and preparing for the cyber attacks. Even today, the focus is too often on technical details without the ability to understand the political context. Ultimately, the decision as to whether a cyber attack is an act of war or something else is a political decision, particularly in cases that fall into the grey area between annoyance and actions that attempt to end the existence of the state.

Passivity in the occurring cyber attacks only encourages opponents more aggression. While assessing the extent of the damage and identifying attack sponsors is especially difficult for cyber incidents, policymakers need to be proactive in determining appropriate response options. Developing a framework with which to respond to cyberattacks allows policymakers to quickly consider solutions and counter with options previously analyzed for merit and possible consequences. Identifying in advance an appropriate response could prevent the state from mistakes that could unintentionally jeopardize political, economic, intelligence, and military interest. Policymakers should also clearly understand also the costs (such as the risk of escalation) associated with each response. The response will have an impact on a country´s diplomatic relations, reputation, and military and intelligence operations.

The increase in state-sponsored cyber attacks is partly the result of a perception that there's not a significant "price to pay" for such attacks. The OPM hack case indicates that there is significant pressure to respond "in some way". However, protocols for responding to state-sponsored national security threats are unclear for cyber attacks, which should be understood as a lack of power in cyber domain. Given the likely pressure governments will feel to respond to cyberattacks, policymakers need to develop a response framework before a disruptive or destructive cyber incident occurs. Although each response will be case specific (it´s situational dependent), a framework will enable policymakers to quickly consider their options. But even if policy response models are created it

does not mean that they will be used accurately. In politics – in cyberpolitics – *there will always be flexibility depending on both current decision makers and ambiguity of the situation*. The framework is also different in each state, because each state has its own cultural, political and military characteristics, so each state should develop its own policy response framework. What you would recommend in one scenario in one country may not be what you would recommend in another.

The need for establishing boundaries in cyberpolitics is critical, without which nations leave their borders and critical systems open to cyber attacks from foreign actors with impunity. There are plenty of different diplomatic, informational, military and economic ways to respond and each state must consider which suitable ways are for them in each attack. One key issue is to consider either physical or cyber response – or both of them together. There is also a possibility for covert response: not to make effects public, and no claim is made.

Covert action may be preferred especially in response in cyberspace as a decision regardless of the strategic and legal consequences. The importance of creating response levels for state-sponsored cyber attacks is two-fold: it provides a framework for deterrence against adversaries and it provides a means to recognize and respond to cyber attacks as they occur. As a benefit, it would also provide a framework for allied countries to create similar network initiatives promoting greater international cooperation, which is a necessity in cyberspace.

The cyber response framework of the state is also an integral part of state´s cyber deterrence. No deterrence theory could succeed without retaliation. In the absence of retaliation, there is no incentive for opponents to refrain from attacking. Deterrence is often the threat to use force in retaliation for an attack.

The response framework (when declaring it publicly) is one way to signal where the lines are the other side should not cross. There has to be muscular in cyberpolitics that would include demonstrations and threaths of retaliatory cyber attacks against other states in a bid to create deterrence similar to the Cold War-era strategic nuclear deterrence. Such strategic logic underlies the state´s declaratory postures, putting adversaries on notice that they should expect even a possible kinetic-military response to some cyber attacks. By thinking externally about the expectations of others, a legal right of armed self-defense might contribute to deterrence by establishing and communicating more emphatically and clearly red lines associated with self-defensive threats. It helps to signal to others thresholds beyond which they should expect a response.

In practice, responses and reactions to cyber attacks will probably involve high levels of secrecy. The perpetrators of cyber attacks may try to keep their responsibility and methods secret. Defenders too, may be reluctant to disclose details or even the very existence of cyber attacks, whether to protect secrets about their

vulnerabilities and defenses, prevent public panic, avoid political embarrassment, or escape unwanted domestic pressure to take retaliatory actions.

Even if the importance of the response model against cyber attacks is emphasized in this paper, cyber attacks and cyberpolitics should not be treated in isolation from the other domains. It is unlikely that state-sponsored cyber attacks occur only as standalone operations. The ability to integrate cyberpolitics – and cyber power – into a broader concept is going to be key. Holistic approach to cyberpolitics is needed, and especially the understanding of the increasing converge between cyber and physical worlds. As long as physical and cyber domains being treated as separate, there is little hope of securing either one, or increase power. The convergence of cyber and physical security has already occurred at the technical level and it is vital increase the strategic understanding on the intertwining physical-cyber security environment in order to succeed.

References

Aspen Institute and Intel Security (2015). Critical Infrastructure Readiness report, Holding the Line against Cyberthreats. July.

Bronk C and Tikk-Ringas, E (2013). “The Cyber Attack on Saudi Aramco”, Survival: Global Politics and Strategy, April-May, pp 81-96.

Choucri, Nazli (2012). "Cyberpolitics in International Relations," Oxford Companion to Comparative Politics, ed. Joel Krieger, Oxford University Press, New York, pp. 267-271.

Department of Defense (2015). The DOD Cyber Strategy, April 2015. [online, accessed 18 January 2016] http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Eberle, Christopher J (2013). “Just War and Cyberwar”, Journal of Military Ethics, Vol. 12:1, 54-67.

Feakin, Tobias (2015). “How to Respond to a State-Sponsored Cyber Attack”, Defense One, 28 August.

Garrie, Daniel (2015). “The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors”, Reuters, 13 August [online, accessed 15 January 2016] http://legalexecutiveinstitute.com/the-limited-options-for-a-corporation-dealing-with-cyber-hostilities-by-state-actors/

Gertz, Bill, (2015). “Intel Assessment: Weak Response to Breaches Will Lead to More Cyber Attacks”, The Washington Free Beacon, 28 July [online, accessed 20 January 2016] http://freebeacon.com/national-security/intel-assessment-obama-admin-response-to-cyber-encourages-more-attacks/

Hackett, Robert (2015). “Let´s Get Physical? United States Weighs Options When It Comes to Cyber Attack”, Fortune, 12 May. [online, accessed 15 January 2016] http://fortune.com/2015/05/12/rogers-cyber-attacks-us-response/

Hathaway, Melissa H. and Klimburg, Alexander (2012). “Preliminary Considerations: On National Cyber Security”, In National Cyber Security: Framework Manual, edited by Alexander Klimburg, 1-19. Tallinn: NATO CCD COE Publications.

Healey, Jason (2012). “Beyond Attribution: Seeking National Responsibility for Cyber Attacks”, Atlantic Council, Cyber Statecraft Initiative, Washington, January 2012, pp 1.

Kremer, J-F and Müller B, editors (2014). Cyberspace and International Relations, Theory, Prospects and Challenges, Springer, London, xi-xvii.

Lehto, M and Neittaanmäki, P, editors (2015). Cyber Security: Analytics, Technology and Automation, Springer, London, pp. 34-35.

Lin, P., Fritzsch L. and Rowe, N (2012). “Is It Possible to Wage a Just Cyberwar?”, The Atlantic, 5 June [online, accessed 15 January 2016] http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/

Maurer, Tim (2015). “Cyber Proxies and the Crisis in Ukraine.” In Cyber War in Perspective: Russian Aggression Against Ukraine, edited by Kenneth Geers, 79-86. Tallinn: NATO CCDCOE Publications.

Ministry of Foreign Affairs of the People´s Republic of China (2015). Foreign Ministry Spokesperson Lu Kang's Regular Press Conference, June 15.” [online, accessed 15 January 2016] http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1273205.shtml

Nakashima, Ellen (2015). “Hacks of the OPM Databases Compromised 22.1 Million People”, The Washington Post, 9 July. 9.

Paletta, Damian (2015). ”NSA´s Rogers Calls for More Forceful Response to Cyberattacks.” The Wall Street Journal. January 8. [online, accessed 15 January 2016] http://www.wsj.com/articles/nsas-rogers-calls-for-more-forceful-response-to-cyberattacks-1420763971

Paletta, Damian (2015). ”When Does a Hack Become an Act of War?” The Wall Street Journal. June 13, p. 7.

Roscini, Marco (2014). Cyber Operations and the Use of Force in International Law. New York: Oxford University Press.

Rosecrance, Richard and Guoliang, Gu (2009). Power and Restraint: A Shared Vision for the U.S. – China Relationship. New York: Public Affairs.

Sanger, David E. Sanger (2015). “Countering Cyberattacks without a Playbook”, New York Times, 23 December.

Singer, Peter and Cole, August (2015). “The Reality of Cyberwar”, Politico, 9 July [online, accessed 15 January 2016] http://www.politico.com/magazine/story/2015/07/the-reality-of-cyberwar-119915

Schmitt, M. N. ed. (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, pp. 106-110.

Stewart, Phil (2015). “Pentagon’s New Cyber Strategy Cites U.S. Ability to Retaliate”, Reuters, April 23. [online, accessed 15 January 2016] http://www.reuters.com/article/us-usa-pentagon-cyber-idUSKBN0NE0AS20150423

Timberg C., Nakashima, E. and Douglas-Gabriel, D (2014) “Cyberattacks Trigger Talk of Hacking Back”, The Washington Post, 9 October.

Thomas, Timothy (2014) “Creating Cyber Strategists: Escaping the “DIME” Mnemonic”, Defence Studies, Volume 14, Issue 4, pp. 370-393.

Tucker, Patrick (2015). “NSA Chief : Don´t Assume China Hacked OPM”. Defense One, July 24. [online, accessed 15 January 2016] http://www.defense-one.com/technology/2015/06/nsa-chief-wont-assume-china-hacked-opm/116203/

Van der Meer, Sico and Van der Putten, Frans Paul (2015). US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations. Policy Brief. September. Netherlands Institute of International Relations.

Wester, Thomas (2014). “Just Cyberwar”, Cyber Security Policy and Research Institute, 24 November [online, accessed 15 January 2016] http://www.cspri.seas.gwu.edu/blog/2014/11/24/just-cyberwar

Williams, Brett T (2014). “The Joint Force Commander´s Guide to Cyberspace Operations”, JFQ, 2nd Quarter, pp. 12-19.

Wollf, Josephine (2014). ”How Would the U.S. Respond to a Nightmare Cyber Attack?” Scientific American. July 23. [online, accessed 15 January 2016] http://www.scientificamerican.com/article/how-would-us-respond-nightmare-cyber-attack/

Vormetric (2015). Media Advisory. July 28, 2015. [online, accessed 15 January 2016] http://www.vormetric.com/sites/default/files/2MB/pr-vormetric-wakefield-media-advisory.pdf

Aalto-ST 3/2016

ISBN 978-952-60-6720-9 (pdf)
ISSN-L 1799-4896
ISSN 1799-4896 (printed)
ISSN 1799-490X (pdf)

Aalto University
School of Electrical Engineering

www.aalto.fi

BUSINESS +
ECONOMY

ART +
DESIGN +
ARCHITECTURE

SCIENCE +
TECHNOLOGY

CROSSOVER

DOCTORAL
DISSERTATIONS