Proportional Response to Cyberattacks

Jarno Limnéll

Analysis in recent years demonstrates that government responses to cyberattacks vary widely. Although there has been significant political pressure to "do something," past experiences illustrate that most policy responses are ad hoc. This indicates that 1) response to cyberattacks is still an exceedingly untested phenomenon; 2) cyber domain is a relatively new arena of conflict—especially for the policymakers—and, therefore, special attention should be directed towards it; and 3) more research is needed to understand how nation-states could best respond to cyber hostilities and which instruments should be used. This article analyzes comprehensively how cyberattacks should be treated as a political question and provides a rough framework upon which policymakers can build. The article presents five variables that policymakers need to consider when evaluating appropriate responses to cyber hostilities. Combining incident impact, policy options, and other variables, the framework outlines the different levers of cyberpolitics that can be applied in response to the escalating levels of cyber incidents. The response framework is also an integral part of the state's cyber deterrence.

Keywords: Cybersecurity, cyberattacks, cyber warfare, cyberstrategy, politics, cyberpolitics, response, security, hybrid warfare

Introduction

The US Department of Homeland Security and the Office of the Director of National Intelligence made a major announcement in October 2016. They officially declared that the Russian government directed the attack on the

Professor Jarno Limnéll teaches cybersecurity at Aalto University, Finland.

emails of US persons and institutions, including political organizations,[1] and stated that "these thefts and disclosures [were] intended to interfere with the US election process."[2] The accusation is remarkable in two ways. First, there is the act itself. The intrusion adds a serious political spin to prior intrusions and was a clear attempt to affect and manipulate the US presidential elections by utilizing cyber methods. The hack is also a reminder of how cyberattacks can undermine the conception of sovereignty, create confusion among people, and blur the borders between war and peace. Second, there is the question of attribution. While absolute attribution is a difficult endeavor, in this case, the US intelligence community stated that it was confident that the hacks could have been authorized only at the highest levels of the Russian government.[3] This public and direct political accusation indicates a high level of certainty of the attribution. Russian officials, however, dismissed the attribution as "rubbish" designed to inflame anti-Russian hysteria.[4]

The most important and interesting question followed the two previous ones. What will be the US response to these hacks? As Barack Obama, the former president said, cyberspace is "uncharted waters" where "you don't have the kinds of protocols that have governed military issues, for example, and arms issues, where nations have a lot of experience in trying to negotiate what's acceptable and what's not."[5] Hillary Clinton made it clear that the

1 In July 2016, the WikiLeaks website publicized embarrassing emails from the accounts of the Democratic National Committee (DNC). The hackers gained full access to the DNC network used by the election staff, including emails, memos, and research pertaining to Democrats running for Congress.

2 Homeland Security, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, October 7, 2016. https://www.dhs.gov/node/23199.

3 Intelligence Community Assessment, *Assessing Russia Activities and Intentions in Recent US Elections*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

4 Dmitry Solovyov, "Moscow says U.S. Cyber Attack Claims Fan 'Anti-Russian Hysteria,'" *Reuters*, October 8, 2016, http://www.reuters.com/article/us-usa-russia-cyber-ministry-idUSKCN1280DO.

5 White House, *Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting*, June 8, 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-/.

"United States will treat cyberattacks just like any other attack."[6] Voices in the United States and in the Western world have urged the US administration to respond and make it clear to Russia that a cyberattack on the democratic process will be met with an appropriate response. President Obama confirmed that the United States had been weighing a "proportional response" and a range of responses were available.[7] What does "proportional response" mean in concrete actions? We do not know. The United States had stated that the response "will be at the time of our choosing, and under the circumstances that will have the greatest impact."[8] This is a new situation for the American national security establishment and policymakers. At the time of this writing, President Obama had ascertained that the United States would sanction nine Russian entities and individuals and expel thirty-five Russian diplomats in retaliation for the US election hacking. President Obama also said that the United States would "continue to take a variety of actions" at a time and place of its choosing, some of which will not be publicized.[9]

The interference of the US presidential elections and consideration of a proportional response to the cyberattack is just one example of the subject of this article, and it raises several questions: Why is it important to create a political response framework to cyber hostilities in today's world? What should be taken into consideration when deciding upon a proportional response to a cyberattack? The hacking of the US elections is also a reminder of the urgent need to develop international norms to reduce the possibility of cyberattacks and hostilities in an increasingly digitalizing world.

---

6 Andrew Blake, "Hillary Clinton: U.S. Will Treat Cyberattacks 'Just Like any Other Attack,'" *Washington Times*, October 7, 2016, http://www.washingtontimes.com/news/2016/sep/1/clinton-us-will-treat-cyberattacks-just-any-other-/.

7 Julie Davis and Gardiner Harris, "Obama Considers 'Proportional' Response to Russian Hacking in U.S. Election," *New York Times*, October 11, 2016, http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html.

8 David E. Sanger, "Biden Hints U.S. Response to Russia for Cyberattacks," *New York Times*, October 15, 2016, http://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html.

9 White House, *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*, December 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

Theoretical Basis

The security of cyberspace is an integral part of today's security, warfare, and politics; therefore, it is important to understand that cyberattacks and other activities in cyberspace should not be separated into a stand-alone area without the broader political, strategic, and geopolitical context. For example, in the ongoing war in Ukraine, the cyber component has been an integral part, which is usually understood as the continuation of politics by other means.[10]

Actions are often divided into five levels: policies and goals, strategies, operations (including campaigns), tactics, and tools.[11] Actions at all these levels are important, but security professionals too often concentrate only on tactics and tools in cybersecurity and—most pertinently—from a technological point of view. This article approaches cyber affairs primarily from the political perspective because of the increasing importance of cyber affairs in today's interconnected world and in international politics. For example, NATO has recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.[12] NATO has also created the ability to invoke Article 5 in response to cyberattacks, which is a political decision.

The analysis of cyberattacks in recent years demonstrates that governmental responses vary widely.[13] There has been significant political pressure to "do something," but experience shows that most policy responses are ad hoc. This indicates that 1) response to cyberattacks is still an exceedingly untested phenomenon; 2) the cyber domain is a relatively new arena of conflict, especially for the policymakers, and therefore it needs special attention;

10 This Clausewitzian approach is controversial, but describes how politics and war are intertwined. See, for example, Mary Kaldor, "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?" *Global Policy* 1, no. 3 (2010): 271–281.

11 See, for example, Richard Bejtlich, "Strategic Defence in Cyberspace: Beyond Tools and Tactics," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCDCOE, 2015), pp. 159–170.

12 NATO, *Warsaw Summit Communiqué*, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

13 See, for example, Sico Van der Meer, "Signaling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors," *Clingeldael*, December 2015, https://www.clingendael.nl/sites/default/files/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf.

and 3) more research is needed to understand how nation-states could best respond to cyber hostilities and the instruments that should be used.

As offensive cyber activity becomes more widespread, policymakers are challenged to develop proportionate responses to disruptive or destructive attacks. Several variables, however, should be considered before responding. At the end of this article, a rough framework is presented upon which policymakers can build, offering a kind of end-result analysis. Combining the impact of cyberattacks, policy options, risks, time, attribution, and proportionality, the framework outlines the different levers of cyberpolitics that can be applied in response to escalating levels of cyber incidents.

The Importance of Politics in Cyber Affairs

Testing the Limits

During the past decade, governmental and non-state hackers have become increasingly sophisticated in their attacks on the digital systems upon which states depend for essential services, economic prosperity, and security. Such breaches have threatened critical infrastructure, intellectual property, privacy of users' data, important national security information, and government personnel data. Due to the advances in technology and the increasing dependency on cyberspace, cybersecurity, as well as its need for rules and common approaches, has become an increasingly important issue. At the same time, the concepts of attack, defense, deterrence, international cooperation, and espionage have assumed new meanings. The heightened reliance upon digital infrastructure and its vulnerability to multiple vectors of cyberattacks has led governments and non-state actors to utilize cyberspace for acting out their geopolitical differences and promoting their political objectives. This means also that the value of "non-kinetic warfare" is increasing. Both international and national discussions about cyberattacks and how to respond to them are long overdue, even if the strategic importance of the digital domain is widely acknowledged. The current "political cyber playbook" is still a slim volume, but it expands daily as parts of the world move towards greater strategic use of cyberweapons to persuade their adversaries to change their behavior.

Nation-states and non-state actors currently are testing the boundaries of the "cyber battlefield," and the number of the visible and invisible cyber activities and the level of their sophistication have been increasing. Innovative

ways to utilize cyberspace are being developed and employed. In December 2015, we witnessed the first confirmed cyberattack to take down a power grid, which affected approximately 225,000 civilians in Ukraine.[14] Cyber capabilities (and the will to use them) are reaching a more advanced level, and it seems that we are not sure how to live in this new reality.

The Rise of Cyberpolitics

In recent years, issues related to cyberspace and its uses have catapulted into the highest realm of politics. Previously, cyberspace had been considered largely a matter of low politics, background conditions, and processes. Today, cybersecurity has become a focal point for conflicting domestic and international interests and—increasingly—for the projection of state power.[15]

It is increasingly important to understand cyberspace as a political domain; this is often forgotten or neglected. When considering cyberspace from the perspective of the nation-state, today's topical cyber questions are very political. Like other domains, the cyber domain should be treated primarily as political. When politics is involved, questions of power are always present. For example, in the context of war, the cyber instrument is like land, sea, and air power—a means to achieve a political aim or increase power. Thus, the strategic use of cyberspace for pursuing political goals and seeking a geostrategic advantage has increased.

With the creation of cyberspace and our deepening dependence on it, a new arena for the conduct of politics is taking shape; moreover, we may be witnessing a new form of politics. This process is described as "cyberization,"[16] which refers to the ongoing penetration of all political fields by different mediums of the cyber domain. Therefore, the concept of cyberpolitics[17] is useful. Cyberpolitics refers to the conjunction of two processes: (1) those

14 E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

15 Jelle Van Haaster, "Assessing Cyber Power," in the *Eighth International Conference on Cyber Conflict: Cyber Power*, eds. N. Pissanidis, H. Rõigas, and M. Veenendaal (Tallinn: NATO CCD COE, 2016), pp. 7–22.

16 Jan-Frederik Kremer and Benedikt Müller, eds., *Cyberspace and International Relations, Theory, Prospects and Challenges* (London: Springer, 2014) pp. xi–xvii.

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

processes pertaining to politics regarding the determination of who gets what, when, and how; and (2) those processes using cyberspace; that is, an arena of digital interactions. In the cyber and physical arenas, politics involves conflict, negotiation, and bargaining over the mechanisms, institutional or otherwise, to resolve contentions over the nature of core values in an authoritative manner. Thus, cyberpolitics is tangible when nation-states consider proportional responses to cyberattacks.

Cyberpolitics is employed across the world largely by academics who are interested in analyzing the use of cyberspace for political activity as well as its breadth and scope. Although cyberpolitics is present at both national and international levels, both cyberpolitics and the cyber domain have created new conditions that do not have clear precedents, even if cyber issues are at the core of the foreign and security policies of nation-states. In the coming years, we will have actual cases that will reveal the true content of cyberpolitics. At that point, we may then return to using the concept of politics—of which cyber affairs are integral—without the need to emphasize the concept of cyberpolitics. Indeed, the cyber domain is no different from the conventional frames of politics.

Global Cyber Norms Are Still at an Early Stage

In 2015, a group of governmental experts at the United Nations tried to develop some rules in the field of information and telecommunications in the context of international security.[18] The report significantly expanded the discussion of cyber norms, rules, and confidence-building measures. The group recommended that states cooperate to prevent harmful cyber practices and should not knowingly allow their territory to be used for damaging international acts using information and communications technologies (ICT). One important recommendation was that a state should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. Even if the report emphasized that "making cyberspace stable and secure can be achieved only through international cooperation" and necessitates that states take appropriate measures to protect their critical infrastructure, it did not give any guidance

18 United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," July 19, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

how to respond especially to state-sponsored cyberattacks. Furthermore, the report stated that it may be insufficient to attribute an attack to a specific state based on the fact that the cyberattack originated in that state's territory or was launched from its ICT infrastructure.[19]

States retain the inherent right to self-defense under Article 51 of the UN Charter when faced with an imminent threat. State behavior in cyberspace should therefore be in line with the UN Charter; however, the challenge of attribution and the understanding of the extent of damage by a cyberattack may complicate the situation. The right to self-defense, including the use of force, would apply if a cyberattack reaches the level of an "armed attack"; yet, the legal debate on what constitutes an armed attack in cyberspace has only just begun. It is conceivable that harmful cyber hostility attributable to a state amounts to a violation of the Article 2 (4) of the UN Charter, given its character and effects.[20] This leads to the question of how to evaluate the impact of cyberattacks, especially if they do not cause physical damage.

A cyberattack does not necessarily have to cause physical damage for it to be considered serious. Possibly due to the long tradition of physical security, physical destruction is strongly emphasized, and it is also easier to observe any physical consequences. The old way of thinking is that a "severe cyberattack" should involve physical destruction, including death and damage to critical infrastructure. However, as we become increasingly dependent on data and non-kinetic assets, could the manipulation of health or financial records, for example, be treated with the same level of severity as physical consequences?[21] Moreover, is there a difference between the manipulation of banking data or health-care data, as the former potentially could result in severe economic disruptions and the latter in death at its extreme? The answer is ambiguous. Moreover, it is unclear what a "major" cyberattack means in practice. It needs to be understood that the answer to the question, whether or not a cyberattack is an act of war, is a political decision and not a conclusion.

---

19 Ibid.

20 "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."

21 Jarno Limnéll and Charly Salonius-Pasternak, "Challenge for NATO—Cyber Article 5," Briefing Paper, Center for Asymmetric Threat Studies, Swedish Defense University, June 2016.

Five Variables

In determining appropriate responses to a cyberattack, policymakers need to consider the following five variables—questions that must be answered before responding.

Who Did It? Attributing a cyberattack to its sponsor—the state or non-state actor behind the attack—remains a significant challenge as it requires effective measures and the ability to identify the perpetrators behind the attack. The problem of attribution is exceedingly complex and not always solvable. Cyberspace allows for a great deal of anonymity, and attacks can be routed through servers all over the world to mask their origin. Misattributing a cyberattack could lead to a response directed at a wrong target. When considering proportionate response, policymakers should understand the level of confidence they have in attributing the attack.[22] For instance, if the level of attribution is low, decision makers will be limited in their choice of response, even if the severity of the attack is high. Governments need to calculate the costs that would incur if they wrongly attributed an attack and consider the potential costs of escalation. Thus, the degree of attribution influences the action taken.

The ability to attribute an attack to a specific source is important for maintaining credibility and ensuring legitimacy at home and abroad. The challenge is that sufficient proof of attribution may be gathered via "secret intelligence data sources" or obtained from "friendly nations," yet the state does not want to publicly reveal these intelligence sources. Releasing at least some proof of attribution is necessary, if the state wants to build international legitimacy for the retaliatory actions it takes.

Attribution involves many aspects, including technical, legal, and political. It is a multi-dimensional issue that requires an analysis of multiple sources of information, including forensics, human intelligence reports, signals intelligence, history, and geopolitics. As Rid and Buchanan argue, attribution is an exercise of minimizing uncertainty on three levels: tactically, attribution is an art as well as a science; operationally, attribution is a nuanced process instead of a black-and-white problem; and strategically, attribution

22 Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident," Council on Foreign Relations, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

is a function of what is at stake politically.[23] Successful attribution requires a range of skills at all levels, careful management, time, leadership, stress testing, prudent communication, and recognizing limitations and challenges. Even if attribution capabilities have increased due to the great interest of security experts on all three levels, the conclusion of the attribution in order to respond is always a political decision.

What is the Impact? Policymakers need to understand the extent of the impact of a cyberattack, as it determines the type and level of response. How harmful the attack has been to national security and society, what kind of services are affected, and whether the attack has caused a significant loss of confidence in the country's reputation are just a few of the questions concerning the effects of cyberattacks. It can take weeks, if not months or years, for computer forensic experts to ascertain accurately and conclusively the extent of the damage done to the target organization's computer networks. For example, it took roughly two weeks for the Saudi authorities to understand the scope of the damage of the Shamoon incident, which erased data from thirty thousand Saudi Aramco's computers. Companies or governmental organizations also sometimes only realize that they have been hacked months or years after the attack. Clearly, it is easier to assess the physical impact of an attack.

When the effects of a cyberattack are not always clear, it is hard for decision makers to determine if the cyber hostility is at the level of an attack and if it requires a response. Many examples of cyber infiltration fall short of their purpose, qualifying rather as nuisance activities or even garden-variety espionage.[24] The challenge with calculating proportionality in the cyber context resides in the speed and covert nature of the cyberattack: it is difficult to establish the magnitude and consequences of a cyberattack. Information to understand the effects can also be difficult to acquire; for example, financial institutions and private companies may be reluctant to provide information about the damage suffered because of business confidentiality.[25]

---

23 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2014): 4–37.

24 James Stavridis, "How to Win the Cyberwar against Russia," *Foreign Policy*, December 12, 2016, http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

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

Which Instruments Can be Used for Response? When considering a proportional response to cyberattacks, the decision is always about the options available to the state. It is said that every nation-state can respond using at least four instruments: diplomatic (i.e., foreign policy instruments such as diplomatic communication, warnings, and sanctions), informational, military, and economic.[26] Policymakers need to consider the full range of responses at their disposal, from a quiet, diplomatic rebuke to a military strike. There is no reason to believe that cyber hostility of any form directly requires a proportionate cyber response. The response does not need to be limited to cyberspace, since nothing bars the state from using other means, although each carries its own political risks. The US Defense Service Board has even suggested that in case of the largest possible cyberattacks, the United States should not rule out a nuclear response.[27] It is usually argued that kinetic responses should be only permissible if the attack has intended lethal effects, causes human suffering or loss of life, or if human rights are directly violated.[28] In increasingly digitizing societies, this is too narrow of an approach, as argued earlier in this article. Currently, however, it becomes difficult to justify kinetic military response to a cyberattack that does not cause physical harm in the conventional sense.[29]

The key issue is to consider which cyber or physical (or other) countermeasures can be used as part of the nation-state's "response arsenal" and which measures should be used in each case. This is a question of the lever of national power at a state's disposal and willingness to use it. Response to cyberattacks may be delivered overtly or covertly. If cyber methods are used, a covert response can be difficult to develop quickly unless the government has already prepared its capability against a specific target, which likely involves prior cyber espionage in order to understand

26 Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," *Defence Studies* 14, no. 4 (2014): 370–393.

27 Department of Defense, Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA569975.

28 See for example, Thomas Wester, "Just Cyberwar," Cyber Security Policy and Research Institute, November 24, 2014.

29 Patrick Lin, Neil Rowe, and Fritz Allhoff, "Is it Possible to Wage a Just Cyberwar?," *Atlantic*, June 5, 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-justcyberwar/258106/.

the target's vulnerabilities. A covert response also does little to warn other countries. An overt cyber response also can be unappealing as states may lose the ability to launch similar cyber responses against other targets and will more likely generate a counter-response. If the response is visible to the public, it should also be accompanied by a narrative of justice, and not of revenge. States may also choose to outsource their responses to proxy hacker groups; in doing so their control over the response may be limited, which could lead to escalating actions.

What Are the Policy Guidelines? Policymakers need to consider the current national security and cybersecurity strategies, which describe the general policy guidelines of the state regarding the political willingness to act and to leverage power. If the state is a member of international alliances and organizations, their policy guidelines must also be considered when formulating the proportionate response. Otherwise, the state can be accused of not following the agreed-upon and shared policies. As mentioned before, cyberspace is not immune to the legal norms that require nations to respond proportionally to an attack.

When a cyberattack occurs, it is possible for policymakers to overreact. Several cyber experts have estimated that overreaction is very real, and decision makers should weigh the possible escalation carefully before responding. As Libicki argues, decision makers should understand what is at stake; that is, what it is that they hope to gain by responding with a given method.[30] Cybersecurity professionals also may have an incentive to trumpet the threat of cyberattacks, which, at times, may heighten the risk of overreacting. Even if political pressure is great following a cyberattack, political prudence is needed. At the very least, a certain level of restraint should be encouraged. Self-restraint is a concept that is relevant for de-escalating the situation, especially if kinetic response is considered. In general, in order to deter the situation from escalating, the adversary needs to believe that the outcome of escalation will be much worse than that of restraint, which occasionally can be a stronger means of manifesting national power.

30 Martin C. Libicki, "Cyberwar Fears Pose Dangers of Unnecessary Escalation," *RAND Review*, Summer 2013, http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html.

How Urgent is a Response? Time is a relevant issue in politics. The political pressure to respond increases especially when the impact of the cyberattack is acknowledged publicly, and the official accusation of the attacker is announced. Not responding fast enough could mean the loss of face and political credibility. Political rivals would likely also exert more pressure towards "doing something." Therefore, the low level of certainty in attribution may be used as an excuse to do nothing.

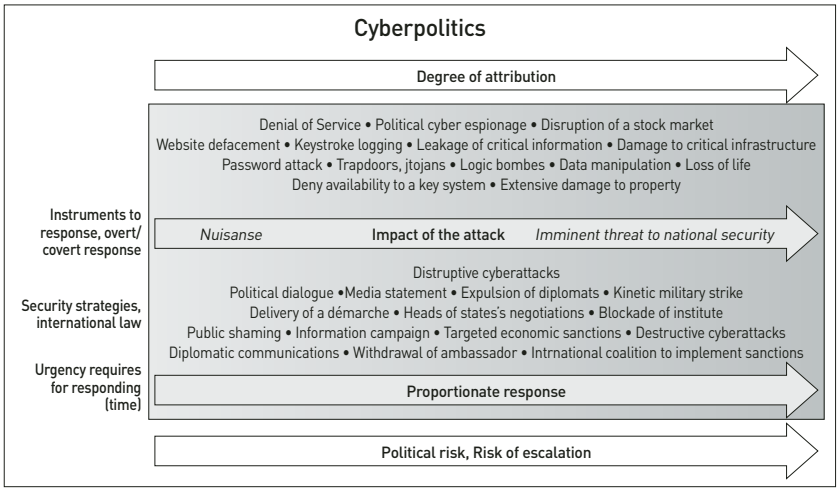
Response Framework

Cyber hostilities provide governments with a complex set of decisions to make, from understanding the level of attribution and the severity of the attack to evaluating proportional response and assessing the risks involved in taking certain courses of action. Decision makers also must assess their kinetic and non-kinetic instruments that can be used in response while time passes and political pressure increases. Passivity in the face of cyberattacks likely will encourage opponents to be more aggressive. Policymakers need to be proactive in determining appropriate response options. Developing a framework for responding to cyberattacks allows policymakers to quickly consider solutions and counter with options that have already been analyzed for merit and possible consequences. Identifying appropriate response in advance could prevent the state from making mistakes that could unintentionally jeopardize its political, economic, intelligence, and military interests. Although each response will be case-specific (situation-dependent), a framework will enable policymakers to quickly consider their options.

Figure 1 below represents a rough example of the framework upon which policymakers should build to determine the potential responses to a cyber hostility before it even occurs. This gives decision makers a starting point for making their own assessments about the course of action to be taken at the time of crisis. Combining the degree of attribution, incident impact, policy options, risks, security strategies, international law, urgency, and proportionality, it outlines the different levers of cyberpolitics that should be applied in response to the levels of escalation and the severity of the cyberattack. The purpose of the framework—while deliberately simplified—is to illustrate the different aspects that policymakers need to carefully analyze when a state considers a range of options and responses to a cyberattack, including the decision to do nothing. According to the framework, the more severe

the cyberattack, the more strongly the response should be. The framework illustrates the impact and severity of a cyberattack, with website defacement at one end of the scale and loss of life at the other. This is analyzed against the level of response, ranging from media statements to military responses. The options of response can be complemented covertly and/or overtly with different instruments. Across the response spectrum are inherent political and legal risks associated with each decision, and risks increase as the level of the response does.

Figure 1: Political Response Framework



As Feakin argues, policymakers should clearly understand the costs associated with each response.[31] Each response will have an impact on the state's diplomatic relations, reputation, power, and military and intelligence operations. Implications need to be understood before a response is chosen. Assessing options will require input from relevant government agencies, as well as private-sector companies, whose operations and businesses could be affected by the response.

The framework should not be interpreted as strict political "redlines" for certain responses. Two sides should be considered when possibly setting

31 Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident," Council on Foreign Relations, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

redlines concerning cyber hostilities. On the one hand, redlines invites adversaries to act below the line, thinking that they have immunity or low political risk in carrying out their cyber operations. Redlines can also push states into the corner so that they are compelled to respond when the line is crossed in order to preserve their credibility. Presumably, states do not want to be too precise about sharing potential responses with the public. On the other hand, setting redlines is a strong message of deterrence to a state's adversaries and lets them know that the state will respond if they cross the line. A certain degree of imprecision may be politically the best solution: the state announces that there will be a response, but it does not reveal the details beforehand.

Conclusion

The role of the cyber domain is increasingly shaping the global security environment and power dynamics between states and other actors. At the same time, cyber capabilities are reaching a more advanced level. We have entered an unstable and suspicious era, and we have done so without a clear roadmap of tested political fundamentals. States are trying to navigate the bounds of acceptable and proportionate responses when faced with confrontational cyber hostilities. Political understanding and commitment is needed more when states are trying to determine the proportionate way to respond to different cyber hostilities. In cybersecurity, the focus is too often on technical details without understanding the political context. Ultimately, the decision as to whether a cyberattack is an act of war or something else is a political one, particularly in cases that fall into the gray area between annoyance and actions that attempt to end the existence of the state. Operating in today's "unpredictable hybrid security environment" requires more political expertise and preparation in cyber issues. Undoubtedly, the significance of cyberpolitics will increase in the coming years. Moreover, policymakers will be forced to re-conceptualize "cyberwar" or "cyber conflict" as a form of "hybrid war" that is contested even during peacetime.

Protocols for responding to cyber hostilities are unclear and should be understood as a lack of power in cyberspace. This article introduced a political response framework that provides a starting point for governments and decision makers to build their country-specific frameworks. Given the likely pressure that will be exerted upon governments to respond to cyberattacks,

policymakers need to develop a response framework of their own before disruptive or destructive cyber hostilities occur. The framework presents the main variables that should be taken into consideration when formulating a response to a cyberattack. The framework also encourages governments to develop their readiness and capabilities in order to obtain answers to the questions presented in the framework—before deciding how to respond.

Even if a political response framework is created, it does not mean that it will be used accurately. One reason is that new methods to utilize cyberspace are being developed all the time. In politics—and in cyberpolitics—there will always be flexibility depending on both the current decision makers and ambiguity of the situation. As each state has its own cultural, political, and military characteristics, all states should develop their own policy-response frameworks. What is recommendable in one national framework may not be so in another.