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

Understanding and Countering Cyber Coercion

Quentin E. Hodgson
RAND Corporation
Santa Monica, California, United States
qhodgson@rand.org

Abstract: The past decade has seen the rise of cyberspace as a topic of popular, political and scholarly discourse, from the highest reaches of government to the movie screen. States are grappling with how to address the rising tide of cyber threats to their economies, to their citizens' personal information and increasingly to political and social cohesion. States are using cyber capabilities as a tool of statecraft to achieve political objectives. This paper seeks to develop an understanding of how states use cyber capabilities to coerce others for political objectives. Cyber coercion is defined as the use of cyber capabilities to compel an opponent to undertake an action it would not normally wish to perform and avoid an undesirable outcome. The paper seeks to address: how a state can employ cyber capabilities to compel another state (or non-state actor) to accommodate its ambitions; how cyber coercion might take place; and ways that the United States and its partners can recognize, respond to and counter attempts at cyber coercion. The paper examines the use of cyber operations by North Korea and Russia in recent years as part of their broader strategies to exert influence over their neighbours, showing how the context in which such operations occur is critical.

Keywords: *cyber operations, coercion, deterrence*

1. INTRODUCTION

The past decade has seen the rise of cyberspace as a topic of popular, political and scholarly discourse, from the highest reaches of government to the movie screen. Military organizations from the United States to the People's Republic of China have grappled with issues from how to address threats emanating from cyberspace to how to integrate cyberspace capabilities into military doctrine (US Department of Defense 2015; Stefan-Gady 2015). In this time, the general public has been exposed to a growing body of reporting on cyberspace issues from the hacking of government agencies, hospitals, public transportation systems and beyond. The US Defense Science Board has issued several reports calling into question both the resilience of military systems to cyber threats (Defense Science Board 2013) and outlining how to deter cyber attacks (Defense Science Board 2017). Government authorities worry that adversaries and others may use cyber means to attack critical infrastructure (Rogers 2017), and more recently the prospect of adversaries undermining democratic processes through disinformation campaigns and even outright corruption of electoral processes has come to the fore.

At the same time, the use of cyber capabilities in a variety of contexts to further nation state interests has grown, from the US' purported targeted operations against Iranian nuclear facilities and North Korea's ballistic missile programme to Iranian-attributed campaigns against Western banks and its regional neighbours. This gives rise to questions about how states are using cyber capabilities as yet another tool of statecraft, including to intimidate, coerce and compel others to do their bidding. This paper seeks to address the question of how states have used cyber capabilities to coerce other states or non-state actors either to pursue courses of action they might not otherwise pursue or to refrain from such actions.[1] More importantly, it compares two actors – Russia and North Korea – which have used cyber operations against their neighbours and others to understand the dynamics of cyber coercion and attempt to isolate factors that indicate when cyber coercion may occur.[2] The paper begins with a discussion of cyber coercion and how it fits into broader deterrence and coercion strategies, followed by an examination of examples from Russia and North Korea. The paper will then suggest some ways that countries can seek to prevent or lessen the impact of cyber coercion.

2. WHAT IS CYBER COERCION?

Any discussion of coercion naturally begins with Thomas Schelling's classic writing on the topic, particularly his seminal work *Arms and Influence*. Schelling described two forms of coercion: active coercion, or compellence, and passive coercion, or deterrence (Schelling 1966). The former involves the active use of force in some form to compel action by another, while the latter involves the threatened use of force to motivate an action or restraint from an action. In reality, the distinction is more of a

[1] The focus of this paper will be on state-to-state interactions, but the author acknowledges Travis Sharp's valuable contribution to the literature that a state may seek to coerce a non-state actor and *vice versa*. See Sharp 2017.

[2] These case studies are intended to inform a broader research project to develop a framework for cyber coercion that ties into response and defensive actions to thwart attempts to coerce through cyber means.

continuum, as some states may combine compellence actions with the threat of more devastating consequences to accomplish their ends. The literature has often focused on the use of force by states, not necessarily because these concepts do not apply to other actors, but rather because the motivation for examining these concepts in the 20th century was to understand the nature of state-to-state relations. As one author recently noted, scholars have often used analogies to more localized conflicts, such as Schelling's reference to teenager hot-rodding and Robert Jervis's reference to village stag-hunting (Sharp 2017).

In recent years, popular, political and academic discourse has tried to find appropriate analogies or comparable historical instances from other domains to explain cyberspace operations, to clarify the concepts of deterrence, or to distinguish cyberspace from everything else (Nye 2011). This paper begins with the premise that, although cyberspace is indeed a man-made domain, its characteristics are more a matter of distinction rather than fundamental difference from other domains when it comes to international relations. States will seek to use cyber capabilities as one tool of statecraft, just as they seek to use other forms of military force, economic power or social and humanitarian influence to further their interests. The same applies to the use of cyber capabilities as a means to exert influence or pressure on others to shape behaviour, deter adverse actions and even compel another actor (either another state, a multinational organization, or even a single individual). As one scholar has noted, coercion is "the use of threatened force, including the limited use of actual force to back up the threat, to induce an adversary to behave differently than it otherwise would" (Johnson, Mueller and Taft 2003). This definition does not require a certain level of force, so cyber weapons do not have to have the same potential impact as nuclear or even conventional weapons to be credibly used to exert influence, nor does the threatened use of cyber capabilities need to be explicit to have a coercive effect.

Coercion in international relations is not the same as it is with, for example, an abduction, although some of the literature uses formulations that more closely resemble abduction than the dynamics of inter-state relations. This is important for two reasons: 1) context is critical to understanding whether coercion is occurring; and 2) the potential for miscommunication between the coercer and the coerced can be significant, even if there is a long-standing relationship between states, as we shall see in the two case studies in this paper. In an abduction, there is usually an explicit demand for action, whether it is demanding a monetary ransom or some other form of compensation such as the release of political prisoners. The scholarly literature describes a logic for the dynamic between coercer and coerced: "if you do not do X, I will do Y" (Borghard and Lonergan 2017). Another form this takes is when a coercive action or threat "demands clarity in the expected result… [and] be accompanied by some signal of urgency" (Whyte 2016). But in reality, the demands are not always so clear. The threat actor may not make a clear threat or identify itself explicitly. To express this difference, we can articulate the theoretical ideal and observed practice as follows:

Theory: coercion = f (clear threat + actor claims responsibility + explicit desired behaviour)

Observed practice: = f (vague threats + implied actor + implicit desired behaviour)

The observed practice is not always a combination of all three; it could involve a clear attribution and explicit desired behaviour, but the threat could be vague. This reality complicates the ability to understand when a state is seeking to coerce another and take steps to counteract or blunt the threat. This paper will return to the differences between theory and observed practice shortly to address whether cyber coercion is successful.

The coercer and coerced may not perceive the messages in the same way (Jervis 1976). Some scholars have noted that cyber coercion is less likely to achieve objectives because the coercive message will signal the threat and allow the coerced to respond or to defend itself, reducing the effectiveness of the coercive measure (Gartzke 2013), but these conclusions are based on a couple of assumptions that do not hold up under scrutiny. Their first assumption is that the coercive measure will be explicit and specific enough to provide the coerced the opportunity to pre-empt the action or prepare its defences. But this is rarely the case, and growing vulnerability to cyber attacks, particularly in more technologically advanced societies, means that the prospective attack surface is so large that adequate preparation is unlikely. The US government, for example, has focused on the protection of critical infrastructure from cyber attack for more than 20 years, starting when President Bill Clinton's Commission on Critical Infrastructure Protection issued its report in 1997 (President's Commission on Critical Infrastructure Protection 1997). The insecurity of critical infrastructure has grown, not diminished, since then.

Their second assumption is that the coercer will signal the means they will use to threaten an opponent. Coercion, however, does not have to state the exact means that will be employed to be credible. The coerced merely has to believe that the coercer has the capability to inflict harm; they do not need to specify "and I will do so with my cyber armies". States are aware of their opponents' capabilities, or they become aware of them over time, and can intuit the potential outcomes. For example, it is highly likely that most states and relevant non-state actors have very little real insight into US cyber capabilities, and in fact may have an inflated picture based on Hollywood movies and the stature of the US civilian technology sector. Couple that with the public belief that the United States probably employed these capabilities to attack both the Iranian nuclear programme and the North Korean ballistic missile programme, and we can see that the actual capabilities that the United States possesses are less important than the perception of them[3] (Sanger and Broad 2017).

This paper is not advancing an argument about the likely success of cyber coercion; several scholars have addressed its apparently low rate of success (Jensen, Valeriano and Maness n.d.; Borghard and Lonergan 2017). A successful attempt at cyber coercion should result from a combination of a successful cyber operation, in which the targeted system or network was disrupted, with a change in behaviour by the coerced. Even in cases where the operation itself achieves its aims, it appears that behavioural changes are few, whether because the actor carrying out the operation overestimated the impact or underestimated the capacity of the adversary to withstand pain. Despite this poor track record, however, states persist in developing cyber capabilities and appear to believe, rightly or wrongly, that the promise of cyber coercion exists. Therefore, we can expect states to continue to pursue coercive actions through cyberspace.

3. NORTH KOREA

Of any state, North Korea is arguably the most likely to employ cyber capabilities as part of a coercive strategy. Despite broad consensus about the country's technological backwardness,[4] the North Korean regime has shown a remarkable astuteness and dedication in investing in militarily relevant technologies, most prominently in its nuclear and ballistic missile programme, but also in recent years in its cyber capabilities (Ball 2017). North Korea has a long history of coercive action, from shooting down a US spy-plane in the 1960s to shelling off-shore islands and sinking a South Korean naval vessel in 2010 (Terry 2013). For North Korea, these actions have largely paid off, resulting in concessions and economic aid from South Korea and the United States as often as more economic sanctions. Sharp (2017) has argued that the North Korean attack on Sony Pictures Entertainment in 2014 was a form of cyber coercion aimed at destabilizing Sony's leadership, imposing costs and seeking to retaliate for perceived insults to the regime with the impending release of a comedy film, *The Interview*, the plot of which is focused on an attempt to assassinate the Dear Leader (Sharp 2017).

The case of North Korea's reaction to the film has been the subject of several analyses, but it is worth briefly reviewing the timeline of events and the broader context in which this case occurred. The proximate cause of the events was the impending release of the film and the North Koreans' strong objections to it. As early as June

[3] One could argue that this is one area where cyber weapons and nuclear weapons are more alike. The United States has not used a nuclear weapon in conflict since 1945 and has not conducted a nuclear test since 1992, but few states if any are likely to doubt the US nuclear arsenal's size or capabilities.

[4] Including reportedly only 28 registered websites. See http://www.bbc.com/news/world-asia-37426725.

2014, the North Korean government condemned *The Interview* in a Foreign Ministry statement and subsequently sent a letter to the UN Secretary General accusing the United States of terrorism and an act of war (Brzeski 2014). After postponing release of the film until December, Sony received emailed demands for money from a group calling itself God'sApstls, followed by a malware attack that resulted in corruption of the master boot records of numerous computers, rendering them inoperable. A group called Guardians of Peace claimed responsibility for the attack and began releasing embarrassing emails and yet-to-be released films in the Sony library (Roman 2014). This was followed by threats of violence against movie theatres and "doxing" of Sony executives through release of internal documents that showed them in a bad light. The North Korean government denied responsibility for the attacks or the threats but referred to the acts as "righteous deed[s]" and speculated that "supporters and sympathizers" of the North Korean regime were involved (Reuters 2014). Sony pulled the movie from theatres, but later reversed its decision after coming under criticism, including from the President of the United States, for appearing to capitulate to threats.

It is important to take a moment to reflect on this point, since if we take the critiques of cyber coercion to heart, the fact that the North denied its involvement would appear to undermine the argument that it was intended as a coercive measure. But the timing of this case is important, as is the context. North Korea clearly indicated its displeasure with the film for several months prior to the events. In the summer, the North Korean Foreign Ministry said "[if] the US administration connives at and patronizes the screening of the film, it will invite a strong and merciless countermeasure" (Brzeski 2014). Totalitarian regimes often fail to understand how western countries operate and conduct their own mirror-imaging. North Korea could very well have believed that *The Interview* was part of an official US government propaganda campaign against the regime. North Korea has a long history of strong rhetoric, but it has also shown itself willing to use force of various kinds with little compunction, whether through directly attacking military targets like soldiers along the Demilitarized Zone and South Korean naval vessels, or civilian targets in the South. From North Korea's perspective, it possibly felt it had conveyed its message clearly and publicly through official channels. The fact that it chose to then follow up on its (failed) coercive rhetoric with cyber attacks through proxies does not detract from the original intent of the threats. The first phase of coercion, which did not explicitly state the form in which subsequent pain would be inflicted, simply failed to achieve the desired outcome of stopping the film, so the North had to escalate from threats to action. At that point, the North Koreans were transitioning from the threat of consequences to seeking to impose those consequences, and who delivered the effects is less important. At the same time, US officials noted that they were not clear on how the threat against the movie theatres was intended to be carried out, which nevertheless did not deter them from treating it as a serious threat (Sharp 2017).

Whether the North Koreans truly believed that the use of proxy fronts (likely for the Reconnaissance General Bureau and the Korean People's Army) would obfuscate the origins of the threats is an interesting question, but currently unanswerable. If the North Koreans had sought to hide their direct involvement, then it is questionable whether it would contribute to the credibility of future coercive threats. That said, North Korean has routinely denied physical attacks, such as the sinking of the South Korean naval vessel *Cheonan* in 2010, when no other credible perpetrators have presented themselves (Terry 2013). It is conceivable that North Korean denies its involvement as a *pro forma* matter as opposed to truly seeking to avoid blame. It also plays to their domestic audience, for whom the regime has to portray itself constantly as the victim rather than the aggressor. Sharp concludes that, while not necessarily achieving all of its aims, the Sony case shows a successful use of cyber capabilities, coupling cyber exploitation (stealing data) with offensive cyber capability to disable computers, coerce Sony's leadership and even lead to the downfall of several senior leaders there (Sharp 2017). Whether the coercive actions were intended to shape other actors is unclear, but North Korea has not limited itself to using cyber to attack private companies. In recent years, it has also employed cyber operations as part of its coercive campaign against the Republic of Korea. Suspected North Korean cyber operations against the South have included targeting the financial, media and energy sectors, as well as government agencies. In some cases, including the attack on a virtual currency exchange in Seoul in May 2017, financial interests may have been the stronger motivation (Perper 2017). The 2013 attacks against South Korean television stations, a bank and bank machines, however, may have been part of an escalatory exchange following a two-day Internet outage in the North (Branigan 2013). These cases are less clearly overt acts of attempted coercion, but they show a willingness to engage in a cyber tit-for-tat and to inflict damage on the South.

North Korea's cyber capabilities are not exclusively retaliatory, nor does the regime likely see them as a replacement for other forms of coercion (Jun, LaFoy and Sohn December 2015). The nuclear and missile programmes are probably still seen as guarantors of regime survival, but cyber capabilities provide a flexible new tool to achieve a variety of ends: theft to improve the regime's finances, espionage and the ability to threaten and inflict pain and damage on its adversaries. The recent cyber events also establish a track record of use that could play a role in future coercive scenarios. Returning to the theoretical construct for coercion (coercion = f (clear threat + attribution + explicit desired behaviour)) we can code the cases as follows:

Case	Threat	Threat Actor Responsible	Desired Behaviour
Sony	Ambiguous	Disputed attribution, but likely North Korea	Clear
South Korea television and banks	Ambiguous	Disputed attribution, but likely North Korea	Unclear

4. RUSSIA AND UKRAINE

Russian cyber activity has gained in prominence, beginning with the denial of service attacks against large segments of the Estonian economy and government in 2007 and as part of the conflict with Georgia in 2008, which some sources have attributed to the Russian government or to patriotic hackers acting on the government's behalf (Davis 2008; Hollis 2010). More recently, the focus has turned to Russian disinformation campaigns and alleged interference in elections in the United States, Germany and France, among others (FireEye January 2017). Russian actors, some more closely affiliated with the government and others playing a more ambiguous role, have established online personas on multiple Internet platforms, including Twitter and Facebook, to disseminate falsified news stories and develop narratives sympathetic to Russia's views (Coats 2017). In the midst of such campaigns, it appears that Russia has also started to use cyber capabilities as a coercive tool. Here we will focus on Russian activity in Ukraine, but this is not intended to downplay or diminish Russian activity in other countries. It is also important to acknowledge that Russian disinformation campaigns, although not the focus of this analysis, could very well be coercive measures intended to destabilize its neighbours and seek to either promote more pro-Russian parties and social movements or motivate current elites to accommodate Russian demands.

The dynamics of Russian-Ukrainian relations are complex and long-standing, which underscores the importance of understanding the context in which the events of recent years have occurred. The Russians have historically seen Ukraine as a part of the border region of Russian territory, rather than as a separate geographic and political entity (in Russian, Ukraine roughly means "on the border"). The Russian military campaign in 2014 to seize Crimea was seen domestically more as a means to correct a quirk of history than an invasion, as Crimea was a gift to Ukraine during Nikita Khrushchev's tenure as leader of the Soviet Union (McCauley 1993). The Crimea also serves as the home port for the Russian Navy's Black Sea Fleet, which makes it strategically important for Russia. Russia's apparent actions to destabilize Ukraine through various means, including cyber operations, supporting proxy fighters and sending military forces into Eastern Ukraine, stem from a desire to maintain Ukraine in Russia's orbit and prevent further integration with the West (Treisman 2016). Ukraine's negotiations in 2013 to conclude a political and trade deal with the European Union also threatened to put Ukraine more squarely in the West's camp.

After then-President Viktor Yanukovich reversed course, protests erupted in Kiev. Police moved in to confront the protesters and violence ensued, resulting in dozens of deaths (Applebaum 2017). In the aftermath of these protests, pro-Russian groups in Eastern Ukraine began to seize control of government institutions, prompting the government to respond militarily. Following the change of President in May 2014, fighting continued and, despite a negotiated ceasefire in February 2015, the conflict continued throughout the year.

In the midst of the horrific fighting and civilian suffering, particularly in Eastern Ukraine, the country suffered the first significant cyber attack on its electric grid in December 2015. The attack affected approximately 250,000 customers for some hours, but appeared to cause no lasting damage despite targeting the Supervisory Control and Data Acquisition (SCADA) controllers in addition to business system workstations and servers (SANS Institute 2016). The malware employed was a set of tools including the BlackEnergy Trojan and the KillDisk eraser and targeted at least three geographically dispersed regional power sub-stations (Greenberg 2017). The impact on the energy sector received the most attention, particularly coming during the winter, but the cyber attacks against Ukraine had also impacted other sectors including media, finance and transportation in the preceding months. Security researchers have attributed the BlackEnergy tool and the actions in Ukraine to the Sandworm intrusion set, which many believe is a Russian hacker group (Hultquist 2016). The Ukrainian government has been more explicit in tying this activity to Russian security services. Attacks on various sectors continued in 2016, including another attack on the energy sector almost exactly a year after the December 2015 attacks that hit the Kiev transmission station; this time the outage lasted barely an hour.

The Russian government has not claimed responsibility for these cyber attacks and routinely denies involvement in cyber operations against other countries, reminding audiences of evidence that the United States in particular has engaged in the widespread use of cyber operations (Russian Ministry of Foreign Affairs 2016). The Russian government did not appear to make explicit demands of the Ukrainian government or public, either in advance of the attacks or afterwards. In the context of the broader conflict, however, the Russian strategy appears to include: establishing facts on the ground through the manoeuvre of military forces and the use of proxies; spreading disinformation to portray the West and pro-western Ukrainians as enemies of the Ukrainian people; and using cyber operations to reinforce that messaging. Cyber operations in this context appear to be intended to broadly destabilize the political and social cohesion in Ukraine.[5] The ultimate outcome, therefore, is predicated on the Ukrainian government acquiescing to Russian influence on the country and halting its integration with the West. In that sense, the coercion appears focused less on seeking to promote specific actions and more towards shaping Ukrainian behaviour for the long term.

[5] There is also speculation that the Russians are using the conflict with Ukraine to ‘test’ its cyber capabilities in a real-world laboratory as a prelude to potential use against other countries such as the United States. Although this may be a collateral benefit, there is little public evidence to support this as the primary reason.

Russian cyber operations against Ukraine show the importance of understanding the context in which conflict occurs. Analysis that examines cyber operations in isolation will fail to identify the implicit outcomes that the instigator seeks, which often go unstated because the parties already know what they are. It is also evident that the Russians are not looking for the Ukrainians to undertake a single, specific action to forestall future cyber coercion, but that it is conducting a broader campaign to prevent Ukraine's integration with the West. The theoretical framework would therefore appear in this case to be as follows:

Case	Threat	Threat Actor Responsible	Desired Behaviour
Russia-Ukraine	Ambiguous	Disputed attribution, but likely Russia	Somewhat clear

5. WHAT CAN WE DO ABOUT IT?

The North Korean and Russian cases demonstrate that states may indeed be using cyber capabilities to attempt to coerce others, but that the ambiguous nature of these campaigns, with their unclear threats, ambiguous attribution and lack of clarity of desired behaviour, makes it less likely that the coercion will succeed, although that has not appeared to diminish their occurrence. That said, these coercive campaigns are not without cost to the victims, which would indicate that some work is needed to counter or mitigate them. Traditional deterrence theory postulates two primary means for response: a threat of punishment for an action that is credible and (one presumes) unacceptable to the opponent, and denial of gains from an action. Professor Joseph Nye (2016/7) has added to these two by postulating that entanglement and normative taboos can play a role. Addressing the threat of cyber coercion will have to account for these mechanisms, but there are practical difficulties in implementing them that need to be addressed. Before addressing these means, however, we should examine how to recognize that cyber coercion is occurring.

The two case studies presented in this paper highlight two key points when seeking to assess whether cyber coercion is occurring. The first is to recognize that the instigator will not always present explicit demands; there may not be the equivalent of a ransom demand. In many cases of state-on-state conflict, the relationship is long-standing and complex, and therefore the nature of the demands may be more implied than explicitly stated. The Sony Pictures case shows a counter-example, where it appears that the demand was clearly stated: do not release the film. But in that case the second point comes to the fore, that the demand will not state explicitly in all cases the form in which threatened consequences will come. In fact, the Sony case included threats of physical harm to movie theatres that never materialised and may have been intended to instil fear with no prospect of the threat ever being carried out; of course, US law enforcement authorities could not take that chance and treated the threat seriously. North Korea may have used the subsequent cyber operations as a means to destabilize Sony Pictures' leadership, as one scholar claimed, but it is just as likely that it presented a tangible way for North Korea to inflict pain when other options were not open to it or would have proved too costly.

These considerations give rise to a set of questions to consider in similar circumstances:

- *Does a state's adversary have demonstrated or emerging cyber capabilities that it should track seriously?* This has implications not only in terms of intelligence collection and analysis, but also in challenging basic assumptions. Both Iran's and North Korea's cyber capabilities took Western governments off-guard because they had simply assumed that these countries did not have the technological capabilities.
- *What is the broader context in which conflict is developing?* Thinking about a country's cyber capabilities in isolation risks missing emerging signals that a coercive campaign is beginning or potentially entering a new phase where cyber operations could occur.
- *Does the coercer have long-standing demands?* Identifying these contributes to understanding what potential outcomes the coercer may seek and could assist in anticipating potential cyber coercive actions.

The threat to impose costs on others for using cyber capabilities has not prevented state use of cyber, though it is impossible to prove an assertion that perhaps current US and Western policies have prevented more egregious actions. It is far more likely that countries such as Russia or North Korea see little reason to fear retaliation at apparently low thresholds of cyber use because the consequences have been spread out over time and have not resulted in loss of life or significant damage to property that would normally invite such a response. The case studies in this paper indicate, however, that there is significant ambiguity around coercive actions using cyber capabilities, which complicates a state's response. States that may be subject to cyber coercion will have to carefully examine the circumstances in which they perceive threats and determine whether a lower threshold for response or even pre-emption may be required. This carries escalation risks, of course, and could even lead to action against an entirely innocent state (at least in the particular situation evaluated).

Given the broad attack surface and the thousands, if not millions, of targets that present themselves in cyberspace, denial of an adversaries' objectives seems an impossible task. The US government identifies 16 critical infrastructure sectors (with "elections" being an ambiguous addition in 2016) that encompass some 1,000,000 owners and operators. Even if a small portion of these are truly critical, such as the list of entities deemed at greatest risk and potentially causing greatest harm (the so-called "section 9" list, referring to the Obama administration's cyber security executive order which was adopted by the Trump administration in its first cyber security executive order), adequately defending them against a vast array of threats is no easy task. That being said, there is evidence that states seeking to coerce others underestimate their capacity to endure pain, and therefore improving resiliency (as opposed to simple defence) is likely a vital component of a counter-coercion strategy (Jensen, Valeriano and Maness n.d.).

In Nye's formulation, entanglement "refers to the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim" (Nye 2016, p. 58). It is possible that this consideration has influenced states such as Russia and China to pursue a less integrated Internet; indeed, Russia has announced plans to create its own form of domain name system to undo its entanglement with the United States (Tucker 2017). Given that, this approach may be useful as a supporting line of effort but is unlikely to prove decisive.

Finally, norms of state behaviour were a central thrust of the Obama administration's work in the UN Group of Governmental Experts (UN GGE) and in its bilateral discussions with the Russian and Chinese governments (Finnemore 2017). For a period of time, this path seemed to have achieved some success, with consensus reports emerging over several years. However, the 2016-2017 UN GGE group failed to achieve consensus and concluded its work without a report on which the 25 participating countries could agree (Korzak 2017). Of course, the establishment of norms as statements of principle are only the first step. Much like customary law, norms gain stature as nations demonstrate through their actions that they are adhering to these norms. The failure of the UN GGE does not in itself signal the death of cyber norms; it simply highlights the challenge of gaining consensus on these issues in a diverse group of countries that do not all necessarily trust each other to negotiate in good faith.

Each of these four proposed approaches has a role to play, but clearly there is no miracle cure that addresses the potential for states to use cyber capabilities to threaten and coerce those whom they seek to bend to their will. The first step is to develop the ability to recognize when cyber coercion could come to pass and seek to head it off, including with explicit warnings and leveraging the four methods Professor Nye identified, with particular focus on improving resiliency in the face of cyber threats.

6. CONCLUSION

This paper has argued that cyber capabilities can indeed be used as coercive tools of statecraft, but recognizing when they may be used and how a state can reduce their impact is no easy task. The context in which cyber coercion may occur is important, as are the capabilities that a state may develop. The increasing commodification of cyber attack tools, the growing legitimate, grey and black markets for these tools and the increasing attack surface all make cyber coercion an increasingly attractive tool for states.

The case studies presented here demonstrate that cyber coercion often occurs in contexts of significant ambiguity. The threat actor may not make an explicit threat, may choose to work through proxies or deny involvement outright, or the desired behaviour may not be clearly stated. In the case of North Korea's attack on Sony, there were vague threats at the beginning from the North Korean government, followed by more specific threats from an apparent proxy. The desired outcome was clear from the beginning, although the coercive campaign ultimately failed to prevent the release of the film. In the denial of service attacks on South Korean television and banking, there was no specific threat, nor a clear claim of responsibility in the immediate aftermath. Indeed, the North Korean government never made a specific demand of the South, but a broader examination of North Korean behaviour over decades indicates that the threats and desired response are long-standing and understood. Similarly, in the Russia-Ukraine context, Russian cyber actors are not explicitly tied to the Russian government, although many observers believe they are at least loosely linked. The desired outcome – Ukraine's drawing back from Western integration and remaining in Russia's orbit – is long-standing. In each of these examples, cyber capabilities appear to have played a role in a broader strategy. Examining them as stand-alone cases misses the broader context in which cyber capabilities are used. More work is needed to develop this context for states of concern to detect, respond and mitigate the effects of cyber coercion.

ACKNOWLEDGMENTS

I would like to acknowledge the work of former MITRE colleagues Peter Sheingold, Cynthia Wright and Mark Peters on grey zone operations that led me to start to explore the concept of cyber coercion. I also want to acknowledge John Parachini, Laura Baldwin, Cynthia Dion-Schwarz and Sina Beaghley for encouraging me to pursue this project and providing support. My thanks to three anonymous reviewers whose comments helped improve the paper immensely. This paper is dedicated in memory

of Shawn Brimley, one of the finest national security professionals it has been my privilege to work with and know.

REFERENCES

Applebaum, Anne. 2017. “Why does Putin want to control Ukraine? Ask Stalin.” October 20. Accessed January 6, 2018. https://www.washingtonpost.com/outlook/why-does-putin-want-control-ukraine-ask-stalin/2017/10/20/800a7afe-b427-11e7-a908-a3470754bbb9_story.html?utm_term=.9fb81.

Ball, Tom. 2017. “Crowdstrike CTO: Theft and destruction are ‘just a few keystrokes’ apart.” *Computer Business Review*. September 29. Accessed December 29, 2017. https://www.cbronline.com/news/cybersecurity/crowdstrike-cto-theft-destruction-just-keystrokes-apart/.

Branigan, Tania. 2013. “South Korea on Alert for Cyber Attacks after Major Network Goes Down.” November 20. Accessed January 6, 2018. https://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack.

Broad, William J., and David E. Sanger. 2017. “Trump Inherits a Secret Cyberwar Against North Korean Missiles.” *The New York Times*, March 5: A1.

Brzeski, Patrick. 2014. “North Korea Files Complaint With United Nations Over ‘The Interview’.” *Hollywood Reporter*. July 11. Accessed December 29, 2017. https://www.hollywoodreporter.com/news/north-korea-files-complaint-united-717943.

Coats, Dan. 2017. “Worldwide Threat Assessment of the Intelligence Community.” Washington, DC: Director of National Intelligence, May 11.

Davis, Joshua. 2008. “Hackers Take Down the Most Wired Country in Europe.” August 21. https://www.wired.com/2007/08/ff-estonia/.

Defense Science Board. 2017. *Cyber Deterrence*. Task Force, Washington, DC: US Department of Defense.

Defense Science Board. 2013. *Resilient Military Systems and the Advanced Cyber Threat*. Task Force, Washington, DC: US Department of Defense.

Elkind, Peter. 2015. “Inside the Hack of the Century.” June 25. Accessed January 4, 2018. http://fortune.com/sony-hack-part-1/.

Finnemore, Martha. 2017. *Cybersecurity and the Concept of Cyber Norms*. November 30. Accessed December 2, 2017. http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870.

FireEye. January 2017. APT 28: *At the Center of the Storm*. Special Report, FireEye iSight Intelligence.

Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38(2): 41-73.

Greenberg, Andy. 2017. “How an Entire Nation Became Russia’s Test Lab for Cyberwar.” June 20. Accessed July 6, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

Hollis, Davis. 2010. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*.

Hultquist, John. 2016. *Sandworm Team and the Ukrainian Power Authority Attacks*. January 7. Accessed January 5, 2018. https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.

Jensen, Benjamin M., Brandon Valeriano and Ryan C. Maness. n.d. “Cyber Compellence: Applying Coercion in the Information Age.” http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/cyber_victory.pdf.

Johnson, David E., Karl P. Mueller and William H. Taft. 2003. “Conventional Coercion Across the Spectrum of Operations: The Utility of U.S. Military Forces in the Emerging Security Environment.” RAND Corporation, Santa Monica, CA.

Jun, Jenny, Scott LaFoy and Ethan Sohn. December 2015. *North Korea’s Cyber Operations: Strategy and Responses*. A Report of the CSIS Korea Chair, Washington, DC: Center for Strategic & International Studies.

Korzak, Elaine. 2017. “UN GGE on Cybersecurity: The End of an Era?” July 31. Accessed September 15, 2017. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

McCauley, Martin. 1993. *The Soviet Union 1917-1991*. London: Longman.

Nye, Joseph S. Jr. 2016/2017. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41(3): 44-71.

Nye, Joseph S. Jr. 2011. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* 5(4): 18-38.

Perper, Rosie. 2017. “North Korea may be behind a massive cyber attack on a South Korean bitcoin exchange that caused it to collapse.” December 21. Accessed January 6, 2018. http://www.businessinsider.com/north-korea-south-korea-bitcoin-heist-2017-12.

President’s Commission on Critical Infrastructure Protection. 1997. “Critical Foundations: Protecting America’s Infrastructures.” Washington, DC.

Rogers, Michael S. 2017. “Statement Before the Senate Committee on Armed Services.” May 9. https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

Roman, Jeffrey. 2014. “Sony Pictures Cyber-Attack Timeline.” December 23. Accessed December 30, 2017. https://www.bankinfosecurity.com/sony-pictures-cyber-attack-timeline-a-7710.

Russian Ministry of Foreign Affairs. 2016. *Comment by Foreign Ministry Spokesperson Maria Zakharova on new threats of sanctions from the United States*. December 28. Accessed January 6, 2018. http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2581641.

SANS Institute. 2016. *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*. January 9. Accessed January 5, 2018. https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

Schelling, Thomas C. 1966. *Arms and Influence*. New Haven, CT: Yale University Press.

Sharp, Travis. 2017. “Theorizing cyber coercion: The 2014 North Korean operation against Sony.” *Journal of Strategic Studies* 40(7): 898-926.

Stefan-Gady, Franz. 2015. “China to Embrace New Active Defense Strategy.” May 26. Accessed December 29, 2017. https://thediplomat.com/2015/05/china-to-embrace-new-active-defense-strategy/.

Terry, Sue Mi. 2013. “North Korea’s Strategic Goals and Policy towards the United States and South Korea.” *International Journal of Korean Studies* 17(2): 63-92.

Treisman, Daniel. 2016. “Why Putin Took Crimea: The Gambler in the Kremlin.” April 18. Accessed January 6, 2018. https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea.

Tucker, Patrick. 2017. “Russia Will Build Its Own Internet Directory, Citing US Information Warfare.” November 28. Accessed November 29, 2017. http://www.defenseone.com/technology/2017/11/russia-will-build-its-own-internet-directory-citing-us-information-warfare/142822/.

US Department of Defense. 2015. *DoD Cyber Strategy*. Washington, DC: US Department of Defense.

Whyte, Christopher. 2016. "Ending cyber coercion: Computer network attack, exploitation and the case of North Korea." *Comparative Strategy* 35(2): 93-102.