2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Hard Power in Cyberspace: CNA as a Political Means

Ragnhild Endresen Siedler
Analysis Division
Norwegian Defence Research Establishment
Kjeller, Norway

Abstract: This analysis is a contribution to the scholarly debate on how cyber power influences international relations. It answers the following question: In what ways can an actor apply CNA to dominate an opponent, and what may restrict him in this effort? It uses Schelling's (2008) argument for dividing power into coercion and brute force, and thus the paper distinguishes between actions that inflict harm and those that impose limitations. Through this approach, it describes the difference between CNA as a means of pure destruction and CNA as a means of forcible accomplishment in order to elucidate different ways of using CNA. This analytical approach aims at generating insight into the nature of CNA threats, which in turn, facilitates development of appropriate responses. The paper argues that defensive cyber strategies and doctrines primarily should focus on CNA as a means of forcible accomplishment. However, it also discusses CNA in the form of coercive threats. It explores this type of power by assessing how the technological and organizational preconditions of CNA apply to severity of consequences and credibility. In particular, two challenges make such threats less credible: unpredictability of consequences, and the ability to make the defender expect that there are more attacks to come. However, one coercive potential of CNA may be in the form of reprisals.

Keywords: *cyber power, hard power, computer network attack*

1. INTRODUCTION

This paper analyzes different ways of using Computer Network Attack (CNA) as a means of power in the context of interstate conflict. Several sources argue for the necessity to develop appropriate responses to hostile actions in cyberspace (U.S. Department of Defense, 2012; NATO, 2014a; Hopkins, 2013). Appropriate responses, however, require insight into the nature of the hostilities in question. In media reports, cyber threats are often described in sensational terms (for example, in Goldman, 2012). However, conveying nuances and an in-depth understanding of the potential power of cyber threats is crucial for identifying appropriate responses.

Here, the term cyber hostility is used as a general term for activities in cyberspace that are in pursuit of an actor's interests and detrimental to his/her opponent. Nye (2004, p.5; 2011, p.11) distinguishes between hard and soft power. Whereas soft power "(...) rests on the ability to shape the preferences of others" (ibid, 2004, p.5), hard power influences peoples' behavior by sanctions. Negative sanctions ("sticks") punish undesired behavior and positive sanctions ("carrots") reward desired behavior. This paper centers on CNA only, and how CNA may be applied to shape circumstances to an attacker's[1] advantage[2] and thus falls into the category of hard power behavior. Hence, the research question is:

> *In what ways can an actor apply CNA to dominate an opponent, and what may restrict him in this effort?*

To answer this question, it may be useful draw on Schelling's (2008) conceptualization of power as either brute force or coercion. This paper distinguishes coercion from brute force according to Schelling's (2008) theoretical argument. Often, CNA threats will occur concurrently, or even in conjunction with, other hostile actions. However, before the interplay between CNA and other actions can be fully explored, it is necessary to gain in-depth understanding of what CNA actually is as an independent means. For the sake of scope and focus, this paper focuses on the latter aspect only. First, it defines how cyberspace relates to the phenomenon of power in the political science sense of the term. Second, it describes how cyberspace's technological attributes constitute preconditions for the political utility of CNA. Finally, it discusses how CNA applies to coercion and brute force respectively.

This paper argues that CNAs shape circumstances mainly by imposing limitations rather than by inflicting harm. CNAs may succeed in being obstacles for military and governmental crisis management, but as a means of coercion, there are critical challenges with respect both to its credibility and to the severity of its consequences.

2. POWER

There is a distinction between the meaning of "cyber power" in political science and how the same expression is understood in military studies. The essence of political science is the analysis of "who gets what when and how" (Lasswell, 1936). In the military context, by contrast, "cyber power" is equivalent to military power projection in the physical domain.[3] This paper discusses cyber power in the political science sense of the term.

From a realist perspective, power is a resource that can be distributed between actors, and thus power is a relative phenomenon in which the enhancement of the power of one actor means a consequent loss to his opponent (Waltz, 2001, p.210; Jackson and Sørensen, 2007, pp.45–46). In the context of conflict, the ability to dominate is a key aspect. Thus, cyber power can enable an actor to dominate opponents. Moreover, conflicts arise as a result of conflicting interest. In

1 I focus on two types of actors: the attacker, who is that actor applying CNA, and the defender, the attacker's opponent and the victim of attack.

2 Computer Network Exploitation (CNE) is also a form of cyber hostility, but, in contrast to CNA, CNE is a type of intelligence collection and not a political means to dominate other actors directly. Hence, CNE is not included in this analysis.

3 For example, the U.S. Department of Defense's (2015) definition of maritime power (projection) as "Power projection in and from the maritime environment, (…)".

such situations, the ability to pursue interests despite actions from opponents is a central aspect. Thus, cyber power implies an ability to achieve one's own interest.

In order to achieve interests, however, power requires actions to transform its potential into results, namely the exercise of power. Hoffman and Graham (2006, p.4) argue that a state of freedom is a precondition for exercising power, and that freedom, in turn, implies having an influence on one's surroundings. Deriving from this logic, cyber power is a phenomenon that empowers an actor to shape circumstances into his/her advantage through actions in or via cyberspace, and thus to pursue self-interests through such actions.[4]

2.1 Schelling: What force can do

Schelling is frequently used by political and military scholars to understand how military means can rationally be applied in pursuit of security objectives. He describes how arms can enable an actor to exercise power. He separates force – how arms influence actors in conflict – into two types: coercion, and brute force. The former is "the power to hurt" and the latter "the power to seize or hold forcibly." Coercion is a latent aspect, which implies that it does not require the use of any means in order to be effective. On the contrary, coercion is most effective when actors comply without any actions being physically carried out (Schelling, 2008, p.10).

Coercion is the main focus in Schelling's (2008) analysis.[5] He argues that this is a form of bargaining power that actors (he mainly focuses on state actors) make use of in order to affect other actors' cost-benefit analysis. This way, coercive power changes and shapes decision-making, and thus is strategic in nature. The ability to influence decision-making, however, is closely related to the ability to inflict harm, or, in the words of Schelling (2008), "the power to hurt":

> "(...) the sheer unacquisitive, unproductive power to destroy things that somebody treasures, to inflict pain and grief–is a kind of bargaining power (...)." (Ibid, p. xiii).

Any threat of harm must be credible. According to Schelling (ibid, p.35), credibility is about communicating that an actor actually intends to carry out hostile actions, as opposed to leaving the impression that it is a bluff. Schelling's focus on strategic decision-making implicitly assumes that such a capability is in place. With respect to cyberspace, however, the technological requirements (as described in the next section) are essential for an attacker's ability to conduct CNA operations, and in the absence of displayed weapons, this paper discusses credibility in the light of what is technologically possible and how that influences the extent to which a CNA

4 There are several definitions of cyber power. Czosseck (2013), for instance, defines this phenomenon as "(…) the ability to act and influence through, and by means of, cyberspace." (Ibid, p.1). Nye (2011, p.123) emphasizes the resource aspect of power and the ability cyberspace provides to gain preferred outcomes. Despite differences in wording, the definition of this paper does not conflict particularly with other relevant definitions of the same term. In this analysis, however, the aspect of "shaping circumstances" is a central aspect. Hence, I use the definition above.

5 Schelling (2008) elaborates on how coercion can be applied strategically in different ways. The distinction between brute force and coercion is theoretical, and the starting point for further elaboration on coercion. The theory developed during the cold war, when strategic air power and nuclear weapons were predominant capabilities. A question, therefore, is whether this provides a useful theoretical basis for analysis of international relations today, and particularly whether it is relevant as an analytical perspective for informing the understanding of cyber power. Despite the cold war context, I argue that Schelling's (2008) theoretical perspective still provides explanations of general value for how arms influence conflicts, and thus may help to elucidate the nature of new types of weapons, including CNA.

threat is convincing.[6] Credibility depends on the defender's expectations (Ibid, p.56). One way in which an actor can enhance his/her credibility is through the application of capabilities. In addition to inflicting "pain and grief" in a specific incident, he can demonstrate that there will be more of such consequences to come, or, as Schelling (2008) puts it when commenting on the nuclear bombing of Japan in 1945: "They hurt, and promised more hurt, and that was their purpose." (Ibid, p.17).

The other type of power, "brute force," is defined by Schelling (2008) as the application of strength in pursuit of self-interest *without* appealing to any other actor's decision-making. It has a kind of "just do it" character. It is the application of capabilities to simply enforce or carry out actions in pursuit of a given objective. Schelling (2008) characterizes this form of power with three key words: strength (in relative terms), skill, and ingenuity. Typical objectives are, for instance, to seize, to penetrate, to occupy, to disable, and to deny access (ibid, p.1). The following quote summarizes the essence of the distinction between brute force and coercion:

> "There is a difference between taking what you want and making someone give it to you (…) between losing what someone can forcibly take and giving up to avoid risk or damage." (Ibid, p.2).

To summarize, brute force is the power to hold or seize forcibly, and CNA in this form of power would be a means of forcible accomplishment, which I in turn interpret as a way of imposing limitations. Coercion, by contrast, is the power to hurt, and CNA in this context would be a means of pure damage, which in turn implies the infliction of harm (ibid, p.8). Table 1 summarizes the distinction between coercion and brute force.

TABLE 1: HOW COERCION DISTINGUISHES FROM BRUTE FORCE

Coercion	Brute force
Inflict harm	Impose limitations
Pure destruction or damage	Forcible accomplishment
The power to hurt	The power to seize or hold forcibly
Coercion is a latent aspect	
A form of bargaining power	
Coercive power changes and shapes decision-making	Application of strength without appealing to any other actor's decision-making

Following Schelling (2008), this paper distinguishes between actions that impose limitations on an actor's capability and those that inflict harm.[7] Deriving from Schelling's (2008) theoretical argument, hard cyber power can be exercised either to influence opponents' capabilities or their

6 Displaying a CNA capability would indirectly point out how a defender could neutralize the threat, as described in more detail in section 4. The contradiction between secrecy of capabilities and the rationality in "show of force," is also discussed in section 4.

7 Correctly, brute force can imply more than mere restrictions or obstacles, as, for instance, in cases of occupation. However, in order to emphasize the contrast with harm, this paper uses the word "limitations," which involves restrictions on a defender's capabilities to a greater or lesser extent, encompassing the whole spectrum of outcomes from disablement and denial of access, to occupation.

decision-making via actions in cyberspace. The next sections elaborate in more detail what such actions in cyberspace can be, and link these actions to their ability to pursue interests.

3. WHAT IS CNA EXACTLY AND WHAT DOES IT MEAN FOR POLITICAL UTILITY?

This paper uses NATO's definition of CNA:

> "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer network itself." (NATO, 2014b).[8]

Maybaum (2013) presents an explanation of what steps a CNA operation consists of, and what consequences it may cause.[9] Several sources distinguish between sophisticated and unsophisticated CNA, based on level of capability requirements (Nye, 2010, p.11; Libicki, 2009, p.154). By sophisticated CNA, this paper means operations that are resource- and intelligence-intensive, as described later in relation to the Cyber Kill Chain; that to a large extent exploit logical vulnerabilities such as zero-day vulnerabilities;[10] and that generally require more effort to circumvent security measures.[11] Less advanced CNAs, by contrast, make use of techniques that are easier to access, such as Denial of Service (DoS) attacks, which could be referred to as digital jamming. Such techniques are often based on off-the-shelf attack tools available on the free market. Though the method of producing a tool might be sophisticated, the attacker can easily apply them without any significant level of expertise.[12] Lindsay (2013) supports a distinction based on sophistication: "The difference in scale between strategic cyber warfare and cheaply available cyber irritants will become more apparent in the matter of offense dominance." (Ibid, p.389).

The level of sophistication an attacker has determines what targets he is able to engage (Libicki, 2009, p.154). Due to the low level of capacity needed for unsophisticated CNA, many actors can acquire a credible but unsophisticated CNA capability. The question is, however, whether that capability is sufficient to influence other actors' capabilities or decision-making.

A sophisticated CNA operation can be described as an array of seven steps: (1) reconnaissance, (2) weaponization, (3) delivery, (4) exploitation, (5) installation, (6) command and control and, finally, (7) actions on objectives (Hutchins et al., 2011). This array is referred to as the Cyber

8 Several sources use other expressions, such as "cyber attack" or "cyber operation." These terms may be confusing, as some include CNE in these terms. For the sake of clarity, this paper consistently uses the term CNA with the definition given above.

9 Maybaum (2013) bases his argument on Hutchins et al. (2011), which is the original source for the Cyber Kill Chain. Because Maybaum's (2013) chapter specifically presents the technologically heavy aspects of the Cyber Kill Chain for a non-technological audience, it is more applicable for this paper, and I mainly use that source here.

10 Stuxnet is frequently mentioned as a highly sophisticated CNA operation. It exploited four zero-day vulnerabilities (Lindsay, 2013). A zero-day vulnerability is defined as "(…) a hitherto undisclosed, exploitable vulnerability (…)." (Czosseck, 2013, p.12).

11 The description of the technological attributes mentioned in this paragraph derives from a meeting with the Norwegian Defence Research Establishment's cyber scientists Ronny Windvik, Torgeir Broen and political scientist Torbjørn Kveberg, Kjeller, 27 November 2015.

12 An alternative to exploiting logical vulnerabilities is social engineering, tricking users to obtain passwords and usernames to access a system or website (Norwegian Defence Research Establishment's scientists, as in footnote 11).

Kill Chain (CKC). Maybaum (2013, p.130) describes the CKC as "a very complex endeavour" in which the intruder is dependent on "deep system knowledge at expert level." This is why sophisticated CNA operations are resource intensive, time consuming, and critically dependent on intelligence. Thus, a sophisticated CNA is difficult to conduct within a short timeframe.

In addition, it is reasonable to expect that the more valuable an asset is to the defender, the more security measures will be in place to protect it. This adds even more challenges for the CNA–developer, and the level of sophistication will have to increase accordingly. Sustaining access to a target over time and awaiting the optimal time of engagement also requires additional effort (Maybaum, 2013, pp.122-126). This restricts how many high-value targets an attacker can simultaneously attack.[13]

Moreover, the malicious code has to be uniquely designed for the target in question (Maybaum, 2013, p.112). This implies that, in contrast to conventional weapons and weapons of mass destruction, "cyber weapons" (or "cyber tools,") used in sophisticated CNAs cannot be stockpiled in huge numbers and used against whatever target emerges at short notice. Hutchins et al. (2011) argue that the defender can conduct several actions to outmaneuver an attacker, and that this is a key advantage in favor of the defender. In other words, the defender too can shape the circumstances to his advantage.

4. COERCIVE POWER IN CYBERSPACE

This section discusses to what extent CNA can influence others' decisions by serving as a "means of pure damage." This implies a discussion of to what extent it can inflict harm. It elaborates on the severity of consequences and then addresses aspects of credibility.

4.1 Severity of consequences

In the public discussion, civilian targets in cyberspace are often conflated with military and governmental crisis management targets.[14] However, in order to make the distinction between harm and limitations more tangible, I distinguish civilian targets from military and governmental crisis management targets. Schelling (2008, pp.8-9) emphasizes the need to specify the level of decision-making being subject to an attacker's influence; that is, whether it is an individual or the strategic decision-maker. As this paper centers on interstate conflicts, it focuses on the level of strategic decision-making. Whereas military and governmental crisis management is by nature instrumental and relates to capabilities, civilians do not represent a capability. Instead, civilians represent that part of an actor where harm materializes as suffering. The rationality for targeting non-capabilities, logically, is not to influence the relative strength between two competitors, but the cost-benefit consideration of the strategic decision-maker and his/her

13 Norwegian Defence Research Establishment's scientists, as in footnote 11.

14 In cyberspace, military and governmental crisis management targets can be information channels between authorities and the population, or communication systems internally in the government to exchange information and coordinate actions. Thus, this can be information infrastructure underpinning the military's or the government's ability to handle the situation effectively.

motivation to avoid risk or damage in the bargaining over competing interests (Schelling, 2008, p.2).[15]

Several scholars (Libicki, 2009; Geers, 2010; Rid, 2013) argue that the impact of CNAs on humans in comparison to other hostile actions such as kinetic attacks and, ultimately, nuclear weapons, are of a low scale. Geers (2010) summarizes this argument: "Cyber attacks *per se* do not cause explosions, deadly heat, radiation, an electro-magnetic pulse (EMP), or human casualties." (Ibid, p.301). This comparison with the consequences of other means of attack is important because it places the effects of CNA in perspective with those of the alternative options an attacker may have at his/her disposal.

An example in which the consequences of CNAs are described in severe terms (for instance, Ottis, 2008), is the Estonia 2007 case. Here, less sophisticated CNA disrupted both private and governmental targets (Tikk et al., 2010).[16] At the same time, there was ongoing disagreement over the movement of a Soviet World War II memorial. Hence, these actions can be interpreted as attempts to influence a political decision.[17] The logic in Schelling's rational choice argument of coercive power is that the costs of giving in must be lower than the costs of suffering a given hostility. Thus, severity is a relative phenomenon. Whether something is considered as severe or not must be regarded in the light of the disputed issue at stake. The cyber hostilities disrupted private businesses and led to economic loss. In addition, they hampered governmental administration services – according to Tikk et al. (2010), a matter of societal security – and Estonia's international communication channels (ibid). Although these actions were described as "the worst-ever DDoS" at that time (Rid, 2013, p.6), Rid (2013) concludes that, although noticeable, the effects remained minor. Tikk et al. (2010, p.25), however, classify the effects as "beyond mere inconvenience," and Ottis (2008, p.2) goes even further, categorizing the situation as a "threat to national security." These assessments of the same consequences illustrate that perception of impact varies to a certain extent.

Despite some variation in perceptions, the question in relation to Schelling's "means of inflicting pure damage," is whether the consequences qualify as sufficient "pain and grief" to influence decision-making. Although the actions resulted in a high number of attacks across Estonian society, encompassing both civilian and governmental targets, and although the effects were noticeable, there are, to the best of my knowledge, no reports of human suffering per se.[18] Kinetic attacks, by contrast, could have led to such outcomes. Therefore, I argue that the consequences in the Estonia 2007 case do not qualify as the severity level of "pain and

15 The principle of distinction in the Geneva Convention, Additional Protocol 1, (International Committee of the Red Cross, 1977) prohibits actors from making civilians the objective of armed attack. This is an indication in itself of the level of severity of such actions, and it also represents a legal restriction on the use of CNA. Notably, the distinction between capabilities and civilians in this analysis is based on Schelling's (2008) distinction between brute force and coercion, and not on legal regulations.

16 Methods used were DoS attacks, Distributed Denial of Service (DDoS) attacks, defacing, attacks on the Domain Name System server, and e-mail and comment spams (Tikk et al., 2010, p.33).

17 There is some uncertainty as to whether the attacker was a state or a number of non-state actors (Rid, 2013, p.7). Due to the scope of interstate conflicts, however, this analysis assumes that the attacker was a state actor.

18 One particular target is worth noting, namely the temporary disruption of the national emergency number, 112 (Tikk et al., 2010, p.21). If citizens in need of public emergency services had not received critical assistance, the consequences could potentially have resulted in human suffering. However, Tikk et al. (2010) emphasize that this number was only briefly blocked, and severe consequences are not reported in this source.

grief" compared to the defender's stake in the conflict, and that the hostilities therefore did not provide the attacker with enough "power to hurt." Consequently, I support Rid's (2013, p.6) statement that, in the end, the attacks did not lead to any significant change in the status quo. Hence, this serves as an example of unsophisticated CNA that did not succeed in producing enough harm to coerce the defender into concessions. If the unsophisticated CNAs on Estonia had any coercive effect at all, it may have been in the form of reprisals. Instead of changing a current decision, reprisal aims at influencing future decisions by imposing a form of punishment (Schelling, 2008, p.79). Although the status quo did not change in the dispute over the World War II memorial, the attacks may have succeed in making resistance costly enough to make both this and future opponents think twice before they again act in a way that is contradictory to the attacker's interests.

In sum, the impact of unsophisticated CNA on people, by comparison to kinetic attack, is relatively low. As an independent tool, unsophisticated CNA faces challenges in making the defender give up, despite civilians being among the victims. However, the coercive impact on future decisions in the form of reprisals may be more relevant.

4.2 Credibility

The threat of sophisticated CNA targeting Industrial Control Systems (ICS) is frequently mentioned in public debate (for instance by Rid, 2013, p.66). The reason is that this kind of control mechanism is almost ubiquitous: in power plants, water plants, electrical and transportation grids, traffic lights, and hospitals, to name but a few examples (ibid, p.67). This dependency represents a source of vulnerability that an attacker could exploit to inflict physical disruption or damage.

Nye (2011) suggests a hypothetical example of a CNA on a civilian target:

> "If a hacker or a government shut down the provision of electricity in a northern city like Chicago or Moscow in the middle of February, the devastation could be more costly than if bombs had been dropped." (Ibid, p.127).

The quote implies that the consequences of such an attack could inflict harm by causing civilian suffering. Given that such a scenario would be technologically and organizationally possible, and assuming that it would be sufficiently severe, would the threat be credible? I argue that there are two main challenges: (1) unpredictability of consequences; and (2) the ability to make the defender expect that there are more attacks to come.

Libicki (2009, p.79ff) argues that, because such attacks depend on exploiting the defender's vulnerabilities, their consequences are more difficult to predict than those of physical attacks.[19] Unpredictability of consequences makes it difficult to convince the defender that he would be better off giving in. What risk or damage is he actually going to avoid?[20] The fact that consequences are difficult to predict may also weaken the defender's belief in the attacker's willingness to use a means in which the outcomes are uncertain. It would also make it less

19 Additionally, the complexity in such systems makes it difficult to predict the consequences of actions (Norwegian Defence Research Establishment's cyber experts, see footnote 11).

20 Arguably, uncertainty is a factor that can increase the perception of a specific risk. However, the type of uncertainty discussed here is rather of a kind that contributes to enhancing doubt instead of fear of consequences.

convincing that the consequences would be sufficiently severe compared with the stakes in question. Contrasting Schelling's (2008) claim that the use of capabilities enhances credibility, Libicki (2009, pp.79-80) argues that, by demonstrating an example the attacker simultaneously reveals the vulnerability on which he bases his CNA operation, and thus indirectly points out how the defender can shape the circumstances to his/her advantage by reinforcing cyber security. When in place, these measures make the attack in question even less convincing as a "promise of more," and the defender is less likely to give in to the attacker's demands (ibid, pp.79-80). Therefore, attempting to achieve coercive power through sophisticated CNA by such a "show of force" is highly challenging.

The uniquely designed code needed for this kind of action also makes it difficult to achieve a convincing "promise of more" expectation. In contrast to air strikes, an actor conducting CNA to take out the centrifuges in the nuclear facility in Natanz does not automatically have the same capability to take out centrifuges in another facility, at least not within the short time required to create a coercive power potential in an ongoing conflict. Arguably, succeeding in such an advanced operation demonstrates a capacity in both organizational and technological terms, which in turn substantiates the possibility of similar actions. However, although the attacker can take some shortcuts, a similar attack would require the development of a new and bespoke CKC designed for the new target. Additionally, the time, resources, and willingness to accept risk of exposure needed for accomplishing all seven steps of the CKC limits how many CKCs an attacker can simultaneously conduct during the course of a conflict. This, therefore, also makes it challenging to produce a "promise of more" expectation in the defender.

Another aspect is the attribution problem, which is often presented as the attacker's key advantage in cyberspace (Rid, 2013, p.139ff).[21] With respect to coercion, however, hiding one's identity is not necessarily an advantage. Libicki (2009) makes the same point: "To coerce, an attacker must signal that a specific set of cyberattacks was meant to coerce." (Ibid, p.80). Instead of denying, he has to *prove* responsibility. Credibility is a factor expressing to what extent the threat of a hostile action is convincing, that is, whether the attacker succeeds in persuading or dissuading an opponent. Logically, in persuading an opponent to give in, it must be convincing that, if he does, the attacker will not inflict the harm the defender gives in to avoid. This is what Schelling (2008, p.74) refers to as "corresponding assurances." If the defender is uncertain of the attacker's identity, how can he assess how the attacker would act in response to his decisions? Therefore, confusing a defender is somewhat counterproductive to the objective of convincing him. Instead, confusion is a form of imposed limitation on crisis management, and can thus be seen as brute force rather than coercion.

These arguments illustrate that a "promise of more" effect is challenging to achieve through sophisticated CNA for two reasons: the tool has to be uniquely designed; and use of such attacks would point out where to close security gaps. In contrast to the use of brute force, the attacker would find it difficult to make use of the attribution problem to his advantage when coercing. If the identity is obscure, the attacker would find it difficult to convince the defender of "corresponding assurances." Instead, the defender may perceive all these obstacles to successful sophisticated CNAs as indications that such threats are bluffs rather than realities.

21 The attribution problem refers to difficulties of tracing attackers in cyberspace.

5. CYBERSPACE AND BRUTE FORCE

How can CNA serve as a "means of forcible accomplishment?" Schelling (2008) summarizes the essence of such a means in three key words: strength, skill and ingenuity. The CKC in itself is interesting. As Maybaum (2013) points out, it requires an optimal match of many details to succeed in all seven steps of the CKC. This, in turn, implies a high threshold for success, particularly for high-value targets. Thus, an attacker will be greatly in need of strength in terms of technological sophistication, skill and ingenuity, in its reconnaissance, social engineering, and ways of accessing networks.

Lindsay's (2013) analysis of the Stuxnet case provides a practical example. He describes how demanding the Stuxnet operation was throughout the different steps of the CKC. His analysis demonstrates that the operation required detailed information on a number of different factors and a highly qualified team with diverse expertise. Hence, sophisticated CNA on high-value targets is an operationalization of the three key words of brute force in their own right, or in the words of Lindsay (2013, p.379): "Stuxnet's technical particulars reveal a devious genius on the part of its developers (…)."

Stuxnet illustrates how a CNA reportedly resulted in physical consequences, in that the speed of the centrifuges in Natanz was manipulated (Lindsay, 2013).[22] The operation is discussed in relation to the international conflict over the Iranian nuclear program and its possible military dimensions. In a nuclear program, enrichment facilities are critical assets. Stuxnet was a covert action that exploited the attribution problem to achieve its objective (ibid). By this, Stuxnet represents a contrast to the exercise of coercive power, which, as argued in relation to credibility, requires proven responsibility instead of deniability. The fact that the attacker did not explicitly appeal to the defender's decision-making (in relation to this particular action), but instead forcibly imposed limitations, underscores that Stuxnet is an example of brute force. Moreover, it is an empirical example of disablement – one of the actions Schelling proposes as types of brute force.

Whereas Stuxnet serves as an example of sophisticated CNA at the strategic level (Lindsay, 2013), Libicki (2009, p.139ff) proposes several ways for how CNA can be used at the operational level of warfare. In particular, he emphasizes the advantage CNA has in taking a defender by surprise. Surprise is a condition imposed on adversaries to gain initiative and make operational advances, or, as Joint Publication 3-0 (U.S. Department of Defense, 2011, p.A-3) puts it: "Surprise can help the commander shift the balance of combat power and thus achieve success well out of proportion to the effort expanded." Therefore, actions causing surprise may have a favorable return compared with their costs. Additionally, disruptions which temporarily incapacitate the defender may provide an attacker with a valuable window of opportunity (Libicki, 2009, p.146). Assuming that such actions are technologically possible, examples of operational use could include blinded sensors, misinterpretations of signals, and weapon system malfunctions (ibid, p.139ff). These are other examples of how CNA can serve as acts of disablement.

22 To what extent the attacker actually succeeded in imposing limitations in the Stuxnet case, however, has been questioned (Lindsay, 2013), but elaborating on this aspect further is beyond the scope of this paper.

Because power is a relative phenomenon, enhancing one actor's "power to seize/hold forcibly," decreases his/her opponent's power to resist or conquer. Therefore, imposing limitations on the opponent's capabilities as illustrated here represents advantages that the attacker can exploit to accomplish his mission.

In 2008, an unsophisticated CNA hit Georgia concurrently with the armed interstate conflict between the country and Russia over the geographical area of South Ossetia. Specifically, this consisted of defacement of key websites, DDoS attacks on government and civilian targets, and spamming of politicians' e-mail accounts (Tikk et al., 2010, p.67ff). The methods used were similar to those seen in Estonia in 2007 (ibid, p.71). However, one noticeable feature of the Georgia case was the targeting of online government communication channels. Tikk et al. (2010) comment on the implications in this way:

> "The Georgian government, reliant on its official websites as information distribution channels, had to look for ways of avoiding information blockade." (Ibid, p.70).

Instead of interpreting this action as an appeal to Georgia's political leadership to change its position in the conflict, the hostilities can be seen as attempts to disrupt its ability to manage the situation, thereby reducing its ability to shape circumstances in favor of its interests. In conflicts, efficient crisis management is a competition between two rivals and their respective decision cycles (Boyd, 1976).[23] Using CNA to disrupt decision cycles, as in the Georgian case by attempting to disrupt communication, and thereby hampering execution of decisions may serve as a useful way to impose limitations on an opponent.[24]

The examples above illustrate how an attacker can use a technological edge to shape circumstances into his advantage without directly harming the defender to concessions. Instead, he uses his strength, skill and ingenuity in cyberspace to "just do it" without appealing to decision-making. This supports the argument that CNA can be used as a "means of forcible accomplishment."

6. CONCLUSION

This paper demonstrates that it is useful to distinguish between CNAs that aim to impose limitations, and those attacks that aim to inflict harm. Sorting threats into these two categories would help analysts and decision-makers to better understand a situation involving a CNA threat. For this reason, the paper also distinguishes between civilian targets and military and governmental crisis management targets.

This paper finds that CNA has the potential to dominate an opponent in the form of "power to seize/hold forcibly," but as "power to hurt" there are challenges with both communicating credibility and causing sufficiently severe consequences. Two aspects represent restrictions in

23 Boyd's (1976) decision-theory resulted in a model describing how organizations conduct decision-making in a circle of four steps: Observe – Orient – Decide – Act, also referred to as the OODA loop.

24 According to Rid (2013, p.8) this attack had limited effect because the Georgian government moved the targeted channel over to a foreign service provider. Despite limited effects in this particular case, it provides a practical example for how CNA potentially can be applied as a "means of forcible accomplishment."

making CNA threats credible. First, uncertainty of consequences makes it difficult to convince the defender that he/she is better off avoiding the risk. Second, it is difficult to convince the defender that there is a "promise of more" of such actions. A more likely coercive potential of CNA is in the form of reprisals, making this and future opponents think twice next time they consider acting in conflict with the attacker's interests.

As a consequence, defensive cyber strategies and doctrines should primarily focus on CNA in the form of a "means of forcible accomplishment," however, keeping in mind that CNA may have a coercive potential in the form of reprisals. Additionally, the results of this analysis may help analysts to nuance the threat picture, and in turn enhance situational awareness among decision-makers.

In relation to the overall phenomenon of hard cyber power, this analysis illustrates how means of power in cyberspace can be applied to influence opponents in the context of interstate conflicts. Given that actions are technologically and organizationally possible, the analysis indicates that hard cyber power primarily has the potential to influence opponents in the form of brute force.

This analysis also illustrates that Schelling's theoretical perspective, which was developed in the context of the cold war and the threat of nuclear weapons, is of general value in facilitating enhanced insight into new types of arms, and even into CNA. Finally, this paper has analyzed CNA as an independent means, omitting the interplay with other actions and how this interplay may change the impact of CNAs. Future work may therefore find it useful to explore this aspect in more detail. Analysing non-state actors and intra-state conflicts in light of Schelling's (2008) theory would also be interesting issues for future research on cyber power.

ACKNOWLEDGMENTS

I would like to express my gratitude to the Norwegian Defence Research Establishment's (FFI) scientists Ronny Windvik, Torgeir Broen and Torbjørn Kveberg for useful and clarifying inputs on technological issues and cyber operations. Additionally, I would like to thank FFI scientist Dr. Tore Nyhamar for advice on political analysis, and for encouraging me to develop this idea into a conference paper. However, the responsibility for any errors or omissions is mine alone.

REFERENCES

Boyd, John R. 1976. "Destruction and Creation." Version 3, September 1976. Available: http://goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf. Accessed: 9 December 2015.

Czosseck, Christian. 2013. "State Actors and their Proxies in Cyberspace." In Ziolkowski, Katharina (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. Tallinn: NATO CCD COE Publication, pp.1–29.

Geers, Kenneth. 2010. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26(3), pp.298–303.

Goldman, David. 2012. “Major Banks Hit with Biggest Cyberattacks in History.” *CNN*, 28 September 2012. Available: http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/. Accessed: 14 December 2015.

Hoffmann, John and Graham, Paul. 2006. *Introduction to Political Theory*. Harlow, Essex: Pearson Education Limited, 1st edition.

Hopkins, Nick. 2013. “British Military at Risk of ‘Fatal’ Cyber-Attacks, MPs Warn.” *The Guardian*, 9 January 2013. Available: http://www.theguardian.com/politics/2013/jan/09/armed-forces-cyber-strategy-criticised. Accessed: 14 December 2015.

Hutchins, Eric M., Cloppert, Michael J. and Amin, Rohan M. 2011. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” Paper presented at the 6th International Conference on Information warfare and Security, George Washington University, Washington, DC, 17–18 March 2011. Available:http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed: 28 October 2015.

International Committee of the Red Cross. 1977. “Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I).” Available: https://www.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp. Accessed: 8 December 2015.

Jackson, Robert and Sørensen, Georg. 2007. *Introduction to International Relations – Theories and approaches.* New York: Oxford University Press, 3rd edition.

Lasswell, Harold D. 1936. *Politics – Who Gets What, When, How*. New York: McGraw-Hill.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation.

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

Maybaum, Markus. 2013. “Technical Methods, Techniques, Tools and Effects of Cyber Operations.” In Ziolkowski, Katharina (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn: NATO CCD COE Publication, pp.103–131.

NATO. 2014a. “Wales Summit Declaration.” Available: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease. Accessed: 9 March 2016.

NATO. 2014b. “NATO Glossary of Terms and Definitions.” (AAP-06 (2014)). NATO Standardization Agency. Available: http://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf. Accessed: 28 October 2015.

Nye, Joseph S., Jr. 2004. *Soft Power – The Means to Success in World Politics*. New York: PublicAffairs 2004, 1st edition.

Nye, Joseph S., Jr. 2010. *Cyber Power*. Boston: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye, Joseph S., Jr. 2011. *The Future of Power*. New York: PublicAffairs 2011, 1st edition.

Ottis, Rain. 2008. “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.” Tallinn: CCD COE. Available: https://www.etis.ee/Portal/Publications. Accessed: 29 October 2015.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. London: Hurst & Company, 2013.

Schelling, Thomas C. 2008 [1966]. *Arms and Influence*. New Haven, CT: Yale University Press. 2008 edition.

Tikk, Eneken, Kaska, Kadri and Vihul, Liis. 2010. *International Cyber Incidents – Legal considerations*. Tallinn: NATO CCD COE.

U.S. Department of Defense. 2011. “Joint Operations.“ Joint Publication 3-0 (JP 3-0).

U.S. Department of Defense. 2012. “Joint Operational Access Concept.” Version 1.0, 17 January 2012.

U.S. Department of Defense. 2015. “Dictionary of Military Terms.” Available: http://www.dtic.mil/doctrine/dod_dictionary/. Accessed: 17 December 2015.

Waltz, Kenneth N. 2001 [1959]. *Man, the State and War – A Theoretical Analysis*. New York: Colombia University Press. 2nd edition.