2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk*

Jason Rivera
Deloitte & Touche LLP
Threat Intelligence & Analytics
Captain, United States Army National Guard
Georgetown School of Foreign Service
Washington, D.C., United States
jhr47@georgetown.edu

Abstract: Achieving cyberdeterrence is a seemingly elusive goal in the international cyberdefense community. The consensus among experts is that cyberdeterrence is difficult at best and perhaps impossible, due to difficulties in holding aggressors at risk, the technical challenges of attribution, and legal restrictions such as the UN Charter's prohibition against the use of force. Consequently, cyberspace defenders have prioritized increasing the size and strength of the metaphorical "walls" in cyberspace over facilitating deterrent measures.

The notion of cyberdeterrence is especially daunting when considering how small states can deter larger, militarily more powerful states. For example, how would Estonia or Japan conduct deterrence through cyberspace against larger regional adversaries with more robust military capabilities? The power disparities between nations of such different military stature are seemingly overwhelming and insurmountable. It is these disparities in cyber power that present conceptual challenges, especially when measuring power in terms of military size, budget, strength, and technological capabilities.

"Power," however, is a broad term that should be considered beyond the military context. This is especially true in cyberspace, where a nation without a strong military can hold a militarily powerful nation at risk, so long as the former is aware of their strategic advantages as well as the critical vulnerabilities of the latter.

Given this reality, this paper shall suspend, or at least cast reasonable doubt on, the notion that cyberdeterrence is either difficult or impossible. Using a deductive method to analyze the components of cyberdeterrence strategy and examine the various challenges involved, this

* All views and concepts expressed in this paper originate solely with the author and do not represent the official positions or opinions of the U.S. Army National Guard, the U.S. Department of Defense, or Deloitte & Touche LLP.

paper introduces a hypothesis on how small, less powerful states can hold large powerful states at risk through cyberspace.

Keywords: *attribution, cyberdeterrence, deterrence, use of force*

1. INTRODUCTION

Cyberdeterrence strategy remains largely unexplored and underdeveloped, due to a limited understanding of how the principles of deterrence can be applied to the cyber domain. Because cyberspace has only recently become an object of national security focus, the development of cyber theory relative to the other domains of warfare is relatively immature. In a broad sense, cyberspace warfighting strategy today is analogous to the growth of air power strategy during the interwar period between World Wars I and II. While the U.S. is actively developing doctrine, mobilizing forces, and allocating resources, there is still much to be done in developing comprehensive cyberspace warfighting strategies.

This paper defines cyberdeterrence as the mechanism through which nation-states can communicate proportionate, reciprocal, and credible military power effects through cyberspace that strategically affect their adversary's decision making calculus. The specific aim of cyberdeterrence is to deter an adversary from conducting hostile actions through cyberspace, although its application could be much broader. For example, a cyberdeterrent could be used to dissuade an adversary from conducting hostile conventional military actions, or even to gain diplomatic leverage.

Four prevailing viewpoints have arisen in the body of work on cyberdeterrence:

1. Cyberdeterrence is difficult but potentially achievable, through the ability to hold the adversary's critical cyberspace security objectives at risk.[1]
2. Cyberdeterrence is difficult and potentially unachievable, due to technical restraints pertaining to attribution.[2]
3. Cyberdeterrence is legally unattainable, due to the UN Charter's prohibition on the use of force and domestic laws that forbid response actions at the substate echelon.[3]
4. Cyberdeterrence is difficult if not impossible to achieve, as any measures taken are unlikely to deter potential adversaries; resources would be better spent pursuing other defensive means.[4]

Acknowledging that these viewpoints outline the challenges of cyberdeterrence, this paper offers the following hypothesis:

A nation-state, regardless of its size or military strength, can achieve cyberdeterrence if it can hold an adversary's critical cyberspace security objectives (CSOs) at risk[a] by communicating its own retaliatory or autonomous cyberspace capability.

[a] The term "hold at risk" should be understood as the means through which nations leverage military capabilities in order to threaten critical national security objectives of other nation-states.

1. If the deterrence capability is retaliatory,
    a. the deterring nation-state need only attribute nefarious actions to the IP space of the adversarial state;
    b. the capability likely would not violate the UN Charter's prohibition against the use of force if it does not violate national sovereignty, does not damage/destroy people or objects, and does not provide weaponry or training to organized actors.

2. If the deterrence capability is autonomous,
    a. the deterring nation-state need not conduct attribution;
    b. the capability may be acceptable if it does not violate the UN Charter's prohibition against the use of force or domestic law forbidding unauthorized network access.

2. HOLDING A LARGE STATE'S CRITICAL CYBERSPACE SECURITY OBJECTIVES AT RISK

A. National Cyberspace Security Objectives

According to realist theory, anarchy forces states to compete for power because that is the best way to achieve security, and achieving security is the only way to ensure survival. This concept is no different in cyberspace, and it applies to the security objectives of nation-states within the cyber domain. In *People, States*, and *Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Barry Buzan cites two principle lenses through which states view their security interests: their ability to leverage military power and their internal socio-political cohesion.[6] In his article 'The Cyber Threat to National Security: Why Can't We Agree?' military strategist and author Forrest Hare argues that these two lenses also heavily affect a nation-state's security objectives in cyberspace.[7] These two lenses divide states into four broad categories:

1. Powerful states with more socio-political cohesion
2. Powerful states with less socio-political cohesion
3. Less powerful states with more socio-political cohesion
4. Less powerful states with less socio-political cohesion

In table 1, Hare sums up states' cyberspace vulnerabilities based on their socio-political cohesion and military strength.

TABLE 1[8]

		Socio-political Cohesion	
		Less Socio-Political Cohesion	More Socio-Political Cohesion
Power	Less Powerful	Destabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDoS and major attacks on critical infrastructure
	More Powerful	Destabilizing political actions in cyberspace	Criminal activities in cyberspace

Hare's table can be used to categorize states according to their greatest perceived threats in the cyber domain, which in turn can be leveraged to hold an adversarial state at risk. Subsequently, these perceived threats indicate a state's most valuable Cyberspace Security Objectives (CSOs). Expanding on this concept, this paper assumes that humanity inherently aspires to be safe, free, generally private, and unoppressed by their governments. CSOs that promote these aspirations are inherently positive, whereas those that detract from these aspirations are inherently negative. States that pursue only positive CSOs do not fear internal insurrection and likely have strong socio-political cohesion. States that pursue negative CSOs likely fear internal insurrection, which indicates a lower degree socio-political cohesion. To classify these objectives further (see table 2), this paper draws from statements by Melissa Hathaway, former director for cyberspace at the U.S. National Security Council, that pertain to security-related aims in cyberspace:

TABLE 2[9]

Positive CSOs	Negative CSOs
1. The promotion of Internet freedom: freedom of speech, content hosting, and browsing	**1. The restriction of Internet freedom:** censorship, controlling content, shaping opinions, forbidding opposition ideas
2. Promoting the availability of services: preventing denial of service, combating malware, etc.	**2. Controlling popular unrest:** restrictions on social media coordination, web-forum gatherings, etc.
3. Combating cybercriminals: identity theft, data breach, hacking, Internet predators	**3. Promoting lawlessness in cyberspace:** crime facilitation, corruption, lack of accountability for actions in cyberspace
4. Combating industrial espionage: copyright adherence, defense of intellectual property	**4. State-sponsored industrial espionage:** copyright violations, intellectual property theft

By understanding these CSOs, one can categorize nation-states and enumerate which equities can be held at risk through cyberdeterrence. This categorization is fundamental to a small state's ability to hold a large state at risk: *understanding the adversary's critical cyberspace security objectives is the most important aspect of leveraging a viable cyberdeterrence strategy*. Consider, for example, the series of cyberattacks in November-December 2014, allegedly

conducted by North Korea against the United States' entertainment industry. By conducting devastating attacks against a company's network, invoking memories of 9/11, and indirectly threatening moviegoers, North Korea, which is militarily less powerful than the U.S., directly deterred the U.S. commercial sector's capacity to exercise freedom of speech.[10] The effect of this cyberspace deterrent was the direct denial of positive CSO one: the promotion of Internet freedom. This paper will continue to expand on this core concept as the various aspects of cyberdeterrence are analyzed.

B. State Categorization

Using the Buzan/Hare model, nation-states can be categorized in terms of socio-political cohesion and cyber power. This paper proposes four such categories:[b]

1. *States with more socio-political cohesion and more powerful cyberwarfare programs:* These states support all positive CSOs, do not support negative CSOs, and can be held at risk if their positive CSOs are threatened.

2. *States with more socio-political cohesion and less powerful cyberwarfare programs:* These states support all positive CSOs, do not support negative CSOs, and can be held at risk if their positive CSOs are threatened.

3. *States with less socio-political cohesion and more powerful cyberwarfare programs:* These states support one or more negative CSOs and can be held at risk if their negative CSOs are threatened.

4. *States with less socio-political cohesion and less powerful cyberwarfare programs:* These states support one or more negative CSOs and can be held at risk if their negative CSOs are threatened.

Drawing on these four categories, table 3 presents a sample of nation-states categorized by cyber power and socio-political cohesion:

TABLE 3

		Socio-political Cohesion[c]	
		Less Socio-Political Cohesion	More Socio-Political Cohesion
Cyber Power[d]	Less Powerful	Bahrain, Belarus, Malaysia, Morocco, Venezuela	Belgium, Denmark, Estonia, Japan, New Zealand, Panama
	More Powerful	China, Egypt, Iran, North Korea, Pakistan, Russia	Australia, Brazil, Germany, India, Israel, U.K., U.S.

b A listing of 77 categorized nations can be found in the appendix of this paper.

c The author defines the term "socio-political cohesion" as a function of civil liberties and political rights, as measured by Freedom House's yearly publication, *Freedom in the World*.

d Cyber power measured as a function of military power, status of cyber warfare capabilities, and relative strength compared to regional competitors.

Table 3 provides a tool for determining an effective way to hold a nation's critical CSOs at risk. Estonia and Japan, for example, both support the positive CSOs and are not known to support any negative ones. Both countries are in the less powerful cyber power category, due to having cyberwarfare programs that fall short of those of their primary regional rivals. History demonstrates that Estonia, for example, can be held at risk by an ability to deny positive CSO number two: promoting the availability of services. This disparity was made evident in 2007 when patriotic Russian hackers allegedly conducted distributed denial of service (DDoS) attacks against Estonian websites, causing a major disruption in Estonian governance. Japan is also vulnerable to large and militarily more powerful actors and, as a result, continually experiences cyberattacks from more powerful entities. In 2014, approximately 25 billion cyberattacks were reported to have taken place against the Japanese government, with approximately 40 percent of them traced to regional rivals.[11] This is an exponential increase from the 2005 total of 310 million, when the first Japanese national cyberattack survey took place.[12]

Those nations in the lower left quadrant of table 3, in contrast, are categorized as strong cyber powers due to their heavy investment in military, intelligence, and law enforcement cyber equities. These nations are unlikely to be held at risk in the same manner as Estonia or Japan, due to their robust capabilities. However, to combat internal socio-political shortcomings, these nations subsequently support negative CSOs. For example the Russian Business Network (RBN) actively supports negative CSO three: the promotion of lawlessness in cyberspace. The RBN is a well-known and relatively blatant supporter of cybercrime that is alleged to have ties to Russian politics; its known nefarious activities include the creation of malware, spam centers, illegal pornographic content, botnets, and monopolization of the market for stolen identities.[13] Two recent and potentially significant examples of such cybercrimes are the point-of-sale identity theft attacks that have been plaguing the retail sector, which were confirmed to have contained the BlackPOS malware with embedded materials that suggest links to a cybercriminal network.[14] These activities and their possible links to politics imply that a deterring entity could hold an aggressor at risk if it could expose the links between criminal and political actors.

Other countries, in contrast, have strict Internet laws and practices designed to control content. For example, according to Section Five of China's Computer Information Network and Internet Security, Protection and Management Regulations, no unit or individual may use the Internet to engage in "making falsehoods or distorting the truth, spreading rumors, destroying the order of society [or] injuring the reputation of state organs."[15] This has led to the widespread filtering of web servers or domain name IP addresses, Domain Name Server redirection, and keyword filtering.[16] These sorts of measures imply that a government that supports negative CSO number one, the restriction of Internet freedom, could be held at risk if a deterring entity were capable of "enabling" unrestricted Internet freedom to the restrictive government's population.

C. Retaliatory and Autonomous Capabilities

The capacity to hold an adversary's critical CSOs at risk is paramount to this paper's hypothesis. Once these security objectives are identified, the deterrer must then develop, communicate,

and, if necessary, deploy a capability that can fulfill its cyberdeterrence objective. In terms of deterrent actions, a nation-state is generally capable of levying either retaliatory or autonomous capabilities.

A *retaliatory deterrence capability* is one that falls in line with Martin Libicki's notion of "the need to develop a capability in cyberspace to do unto others what others may want to do unto us."[17] Employing this capability insinuates a response-focused cyberdeterrence mechanism that threatens the adversary with use of force if it continues to conduct nefarious actions. Retaliatory responses, in general, are problematic on two fronts. First, they require a certain extent of attribution. Precise attribution is problematic with currently available technology and will likely be so in the immediate future. Second, a retaliatory response may require the threat of use of force, which violates article 2(4) of the UN Charter's prohibition against the use of force. These problems will be discussed later in this paper, but it should be made clear that levying a retaliatory capability requires the deterrer to address attribution and legal concerns.

A deterrer also can leverage *autonomous deterrence capabilities*, which are mechanisms that do not require active response or counteroffensive actions to be effective, such as a firewall or a honeynet. At a minimum, a firewall or honeynet will force a nefarious actor to expend valuable time. It is even better if the firewall reports the IP address of those attempting an intrusion, or if the honeynet reveals the attacker's methodologies and tools. Autonomous capabilities, while potentially less effective than retaliatory capabilities, have a lower threshold in terms of attribution requirements and conform more with international legal norms.

Both retaliatory and autonomous capabilities must be communicated to an adversary in a way that effectively demonstrates that the deterrer can harm their CSOs. However, the deterrer must not communicate its capability in a way that allows the adversary to render it useless. An adversary who censors the Internet, for example, must be made to believe, via deterrence communication channels, that the deterrer is able to restrict or eliminate the adversary's capacity to censor the web. Similarly, an adversary state that sponsors industrial espionage must believe that the deterrer has the cyber capability to harm it if it continues to support espionage activities.

3. ATTRIBUTION AND CYBERDETERRENCE

One key challenge in achieving cyberdeterrence is the notion of attribution. The attribution problem has technical and human components, and both can be challenging. Technical attribution includes analyzing malicious code, functions, and packets and then leveraging this analysis to locate the networked node where the nefarious activity originated.[18] Human attribution involves leveraging the results of technical attribution to identify an organization or person responsible for the nefarious activity.[19] In both cases, attribution is not an end in itself but a means for holding the adversary's critical cyber equities and objectives at risk. Because attribution is a means, not an end, this paper disputes the notion that one must unequivocally identify the adversary's location and networks to achieve deterrence. To levy a retaliatory capability, one need only conduct attribution back to the IP space of the offending nation-state,

which is achievable with currently available technology. If using an autonomous capability, the deterring state need not confirm attribution, since the capability will autonomously levy adverse effects against intruding adversaries.

A. Retaliatory Capabilities and Attribution

The nature of state-sponsored cyber activity suggests that attribution can be achieved in tiers. U.S. Senator Sheldon Whitehouse suggests that tiered attribution can be achieved as follows: nation → region → city → group → individual.[20] Cybersecurity firm Mandiant's exposure of Advanced Persistent Threat 1 illustrates this concept. Starting with suspected Chinese state-sponsored industrial espionage activities, Mandiant managed to narrow down the aggressors to → large-scale infrastructure in Shanghai → specific fiber optic infrastructure provided by state-owned enterprise China Telecom → PLA Unit 61398 → specific individuals.[21] This demonstrates attribution for nefarious activities from the nation-state echelon down to the individual. However, to achieve cyberdeterrence a nation-state need not attribute blame to the individual but to the responsible state, thus it would have been sufficient to attribute the nefarious actions back to the country in which the Internet service provider was hosted.

The capacity for a small state to achieve attribution against a large state is especially relevant in the discussion of retaliatory capabilities. Far too often, small states see the inability to gain precise attribution as a non-starter for employing retaliatory capabilities, but this simply need not be the case. In the article 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks,' Jason Healey notes that "analysts often fall into the trap of 'attribution fixation,' the belief that they cannot assess which organization or nation was behind an attack until technical forensics discovers the identity of the attacking machines."[22] Healey adds that "knowing 'who is to blame?' can be more important than 'who did it?' Moreover, attribution becomes far more tractable when approached as a top-down policy issue with nations held responsible for major attacks originating from their territory or conducted by their citizens."[23] It logically follows that nation-states are almost always (wittingly or unwittingly) responsible for cyber aggression ranging from the IP space of their geographic borders. Table 4 juxtaposes a spectrum of state responsibility with historical incidents of cyber aggression.

TABLE 4

Spectrum of State Responsibility[24]	Historical Example
1. State-prohibited: National government will help stop third-party attacks.	In 2002, the U.S. Federal Bureau of Investigation creates a Cyber Division to combat cyber-based terrorism, foreign intelligence operations, and cybercrime.[25]
2. State-prohibited-but-inadequate: National government is cooperative but unable to stop the third-party attacks.	In 2014, a report indicate that the United States, despite having stringent Internet law enforcement measures, is host to approximately 40% of malware serving botnets, more than any other country in the world.[26]
3. State-ignored: National government knows about the third-party attacks but is unwilling to take any official action.	In 2007, "patriotic hackers" conduct DDoS attacks against Estonian state websites.
4. State-encouraged: Third parties control and conduct the attack, but the national government encourages them as a matter of policy.	Around 2007, Iran creates the Basij Cyber Council to organize Iranian civilian hackers under the supervision of the Iranian Revolutionary Guard Corps.[27]
5. State-shaped: Third parties control and conduct the attack, but the state provides some support.	The Syrian Electronic Army, a group that supports the Syrian regime and likely receives some state support, hacks into several news producing entity.[28]
6. State-coordinated: National government coordinates third-party attacks, such as by "suggesting" operational details.	In 2008, Russia sponsors website "StopGeorgia.ru," which encourages the hacker population to engage targets within Georgian web space.[29]
7. State-ordered: National government directs third-party proxies to conduct attacks on its behalf.	In 2005-2007, in an effort to delay the Iranian nuclear program, the United States, under the George W. Bush administration, allegedly initiates an effort code-named Olympic Games,[30] and coordinates with third-party Israeli proxies to plant USB devices in key Iranian nuclear facilities.[31]
8. State-rogue-conducted: Out-of-control elements of government cyber forces conduct the attack.	In 1999, after the accidental bombing of the Chinese embassy in Belgrade, rogue hacker elements from Russia, Latvia, Lithuania, and Serbia conduct anti-NATO cyberattacks.[32]
9. State-executed: National government conducts attack using cyber forces under their direct control.	In 2007, Israeli forces infiltrate Syrian air space and destroy the al-Kibar nuclear reactor by triggering a kill-switch installed in Syrian air defense radar systems.[33]
10. State-integrated: National government attacks using integrated third-party proxies and government cyber forces.	For the last decade, several government entities have used third parties to conduct targeted exfiltration attacks against firms and major industries to enhance their economy and defense industry.[34]

This section demonstrates that the attribution threshold for deploying retaliatory capabilities only requires a nation-state to attribute nefarious actions back to the IP space of the offending state. Even if malicious actors employ proxies in third-party countries to conduct cyberattacks, the third-party nation still has the responsibility to act. Healey once coined the term "Cyber Somalia," which refers to a tendency in the international community to treat cyberattacks "as if every country were Somalia: helpless to restrain attacks from its territory or mitigate their downstream impacts."[35] This is simply not the case. States, especially highly capable and technologically developed states, typically have the law enforcement means to assume responsibility for actions within their borders.

B. Autonomous Capabilities and Attribution

Whereas the physical domain is characterized by variations in the terrain, cyberspace is characterized by environmental variables, including the emplacement of and interaction

between routers, switches, servers, firewalls, and transmission mediums. One central difference from the physical domain is that cyberspace is manmade and therefore can be altered, which is the premise on which autonomous capabilities not focused on attribution can be leveraged.

Autonomous capabilities can support a small nation-state's pursuit of cyberdeterrence if the deterrer correctly conducts organizational characterization and predictive cyberthreat analysis. Organizational characterization will help the deterrer understand the equities that a nefarious adversary may threaten; predictive cyberthreat analysis will help the deterrer understand the tactics, methods, and means the adversary will most likely use. Once a deterrer achieves organizational understanding and can reasonably predict the nature of a cyberthreat, attribution is no longer required, as the deterrer will have the knowledge needed to levy an autonomous capability. Table 5 presents examples of autonomous cyberdeterrent capabilities that do not require attribution.

TABLE 5

Organization	Cyberthreat	Autonomous Cyberdeterrent Capability
Intelligence Agency	Hacktivist conducting website defacement	Firewall with attached intrusion prevention system that conducts reverse IP address look up of nefarious actor; broadcasts location of all proxy IP addresses and actors to law enforcement forces, thereby degrading anonymity.
Host-Nation Military	Adversarial military force conducting offensive operations	Intentionally seed deterrer's network with malware so that when data is exfiltrated back through the ISP of the aggressor country, the ISP's ability to censor the Internet or social media is degraded, thereby hampering the strategic objectives of autocratic states.

4. LEGAL CONSIDERATIONS AND CYBERDETERRENCE

A. Legal Considerations of Retaliatory Capabilities

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is the most comprehensive work outlining the international laws and norms of cyberspace in accordance with the UN Charter. This section of the paper focuses in particular on *Tallinn Manual* Rule 10: Prohibition of Threat or Use of Force: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[36]

Taking into account the *Tallinn Manual*, a deterrer considering using a retaliatory capability will need to comply with two things: the UN Charter's prohibition on the use of force and the non-intervention principle. Compliance is critical, as deterrence actions occur before hostilities begin, and thus, are generally recognized as not covered under the right to self-defense and must not be characterized by the use of force. As for the non-intervention principle, article 2(7) of the UN Charter states that "the United Nations has no authority to intervene in matters which are within domestic jurisdiction of any State."[37] The *Tallinn Manual* states that "the fact that a cyber operation does not rise to the level of a use of force does not necessarily render it lawful

under international law."[38] A good example of crossing the non-intervention threshold is when the U.S. provided training and weapons to the Contras in Nicaragua. Although the U.S. was not directly involved in kinetic operations, in 1986 the International Court of Justice ruled that U.S. actions constituted a use of force.[39]

Table 6 gives examples of what the *Tallinn Manual* would and would not consider state-sponsored use of force.

TABLE 6[40]

Use of Force	Below Use-of-Force Threshold
Cyber actions that kill people or damage/destroy objects	Conducting psychological operations designed to undermine confidence in government or economy
Providing an organized group with malware and the requisite training to conduct a cyberattack	Funding a hacktivist group conducting cyber operations as part of an insurgency
Training an organized group to conduct a cyberattack	Granting sanctuary to non-state actors to conduct cyber operations
Providing sanctuary in addition to cyber defenses for a non-state group	Failing to police territory and prevent launch of cyber operation by non-state actors

In addressing the four retaliatory capabilities listed above in the "below use-of-force" column, a full-fledged cyber power will be unable to levy the "Cyber Somalia" excuse within the international community. This means that granting sanctuary or failing to police a state's territory are not viable options. Moreover, funding a "hacktivist" organization will require leasing control of national-level CSOs to unpredictable and unquantifiable entities, which would defeat the purpose of conducting proportional, reciprocal, and credible deterrence operations. Therefore, to achieve cyberdeterrence using a retaliatory capability while adhering to the *Tallinn Manual*'s guidance on the use of force, deterrers should levy psychological operations within the cyber domain. Psychological cyber operations should be designed to have a widespread effect on the targeted nation's populace while remaining below the threshold of force.

The notion of CSOs was referenced above as the key cyber aim point needed to hold an adversary at risk. Therefore, an examination of the suitability of retaliatory capabilities should be premised on how these objectives are held at risk and whether the retaliatory capability in question crosses the use-of-force threshold. Table 7 presents some retaliatory psychological operations capabilities that could be deployed against adversaries with negative CSOs that would not cross the use-of-force threshold.

TABLE 7

Potential Adversary & Activity in Support of a Negative CSO	Retaliatory Deterrence Capability That Is below Use-of-Force Threshold
A government entity that monitors online content and communications through a centralized location in the regime's telecommunications monopoly.[41]	Enable externally hosted search engines outside of the jurisdiction of a nations ISPs, thereby negating the government's ability to censor web searches.[42]
In response to ongoing protest activity, a government that blocks and degrades content on popular social media websites.	Provide proxy access to unrestricted social media websites, thereby enabling the population's ability to coordinate ideas and protest against the government.
Large government entities known for their heavy concentration of corrupt bureaucrats that are responsible for the facilitation of cybercrime syndicates.	Expose intelligence-related information that provides proof of corrupt relations between government officials and cybercriminals.

Note that a retaliatory capability that does not violate the UN prohibition on the use of force may not necessarily imply that the capability is in compliance with article 2(4) of the UN Charter. Any action that violates nation-state sovereignty or intervenes in domestic affairs may still be prohibited, even if such actions are akin to the national intelligence collection process levied by nations throughout the world. Therefore, levying a retaliatory cyberdeterrence capability requires decision makers to make a conscious decision on their usage and therefore accept the potential of a negative outcome.

B. Legal Considerations of Autonomous Capabilities

If a deterrer is operating at the substate echelon, it is critical that it stays within both international law and the boundaries of domestic law—especially when leveraging autonomous capabilities. There is a strong inclination, particularly in Western law, to outlaw unauthorized access to computer networks, known as hacking. This includes "hack-backs," private companies that attempt to retaliate against cybercriminals in order to deter crime, steal back information, shut down the assailant's network, or seek revenge. For example, 18 U.S. Code § 1030 states that "knowingly access[ing] a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information," is illegal.[43] Given this restriction, it is critical that autonomous cyberdeterrent capabilities not be dependent on gaining unauthorized access.

To abide by domestic law, the deterrer must execute cyberdeterrence functions from within its own network. Thus when the deterrer's network has been compromised, it should implement internally based cyberthreat countermeasures (IBCC), which are designed to autonomously levy a negative response against an adversary.[44] The organization levying an IBCC would be required to act within legal constraints. In the U.S., for example, title 10 (military) and title 50 (intelligence) organizations have the legal authority to employ malware in the execution of their roles.[45] Examples of autonomous capabilities that could be used by those with the legal authority to employ malware appear in table 8.

TABLE 8

Deterring Organization	Adversary	Threatening Action through Cyberspace	Autonomous Deterrence Capability
Intelligence Agency	Rival Intelligence Agency	A foreign intelligence agency conducts operations to exfiltrate valuable national security data.	Intentionally host malware within the deterrer's intelligence agency network; when that malware is exfiltrated to the rival intelligence agency's network, the malware opens up a back door, allowing the deterrer's organization to conduct Computer Network Exploitation (CNE).
Law Enforcement Agency	Organized Criminals	Groups of organized criminals conduct financial crimes against a deterring nation's citizens and corporations.	Flood the Internet with intentionally hosted proxy networks, applications, and web forums that attract users within the organized crime echelons. An example of such a service is the Silk Road, a Tor hidden service designed to allow users to anonymously conduct illicit trade activities online. When those proxy networks, applications, and web forums have gained sufficient bona fides, push Trojan updates to those hosted entities that compromise the computers of the organized criminals and subsequently reveal their location and activities.

Other entities may not have the legal authority to host malware but nonetheless be critical to a nation-state's cyberspace security posture. These include the defense industrial base, information technology, telecommunications, energy sectors, etc. These sectors may be required to levy autonomous deterrents that affect the risk calculus and operational strategy of the adversary, as opposed to infecting the adversary's networks with malware. Examples of such capabilities are presented in table 9.

TABLE 9

Deterring Organization	Cyberthreat	Threatening Action through Cyberspace	Autonomous Deterrence Capability
Defense Industrial Base (DIB)	Intellectual Property Thief	In order to gain a competitive advantage, a foreign military conducts industrial espionage through cyberspace.	Develop a honeynet that includes intentionally seeded and flawed information designed to sow confusion, misdirection, false intent, and deception. For the DIB, honeynets should contain technology/personnel counter-data that is relevant, yet disadvantageous to an adversary.[46]
The Energy Sector	Terrorists	Terrorists seeking to cause chaos attempt to gain access to the electrical power grid by using a sniffer on a network in order to compromise electrical power company usernames and passwords.	Develop and deploy software that would make it so, that for every legitimate login attempt that took place, the software would simultaneously fabricate additional username and password attempts across the network. The aim would be that the employee endpoint terminal itself would be unable to differentiate between the legitimate login attempt and the fabricated login attempt. Login attempts would be transmitted via encrypted channels to a highly secure central processing location, and fabricated login attempts would be sent to another centralized database. If a criminal/terrorist entity were to use fabricated login data to log in to the close network, it would be flagged and thus cue law enforcement authorities.[47]

5. CONCLUSION

This paper has discussed the plausibility of cyberdeterrence and the challenges in achieving it. By breaking down the various challenges, which include the ability to hold the adversary at risk, the notion of attribution, and the need to operate within legal norms, the paper gives credence to its hypothesis that cyberdeterrence can be achieved, and that even small nation-states can achieve it using retaliatory and autonomous capabilities. Small states can levy retaliatory capabilities to achieve deterrence so long as they can attribute nefarious actions to the IP space of the adversarial state and the retaliatory capability does not violate the UN prohibition on the use of force. Alternatively, small nation-states can achieve cyberdeterrence using autonomous capabilities, which do not require attribution and can be leveraged in conformity with article 2(4) of the UN Charter as long as they violate neither the UN prohibition on the use of force nor domestic law forbidding unauthorized network access.

Cyberdeterrence, like conventional deterrence, centers on understanding the adversary's center of gravity, having a threatening capability, and communicating to the adversary the willingness to unleash the capability if a red line is crossed. To position the cyberspace environment to their advantage, cybersecurity practitioners at both the interstate and substate echelons should integrate cyberdeterrence into their defensive plans.

6. APPENDIX

Nation-State[e]	Military Power Index[f] [48]	Presence of Government Sponsored Cyberwarfare Programs[49]	Political Rights[50]	Civil Liberties[51]
Argentina*	2		High	High
Australia+*	4	Yes	High	High
Austria*	3		High	High
Azerbaijan	2		Low	Low
Bahrain	1		Low	Low
Bangladesh	2		Medium	Medium
Belarus	2		Low	Low
Belgium*	3		High	High
Bolivia	1		Medium	Medium
Brazil+*	4	Yes	High	High
Bulgaria*	1		High	High
Canada+*	4	Yes	High	High
Chile*	2		High	High
China+	5	Yes	Low	Low
Colombia	2		Medium	Medium
Croatia*	2		High	High

e The + symbol = strong cyber power relative to adversaries; the * symbol = relatively strong socio-political cohesion.

f 5 = most powerful; 4 = highly powerful; 3 = powerful; 2 = less powerful; 1 = minimally powerful

Czech Republic*	3	Yes	High	High
Denmark*	3		High	High
Ecuador	1		Medium	Medium
Egypt	4		Low	Medium
Estonia*	1	Yes	High	High
Finland*	2		High	High
France+*	5	Yes	High	High
Georgia	2		Medium	Medium
Germany+*	5	Yes	High	High
Greece*	2		High	High
Hungary*	2		High	High
India+*	5	Yes	High	Medium
Indonesia*	4		High	Medium
Iran+	4	Yes	Low	Low
Israel+*	4	Yes	High	High
Italy+*	4	Yes	High	High
Japan*	4	Yes	High	High
Jordan	2		Low	Medium
Kazakhstan	1		Low	Medium
Kenya	2	Yes	Medium	Medium
Kuwait	1		Medium	Medium
Lebanon	1		Low	Low
Lithuania*	1		High	High
Malaysia	3		Medium	Medium
Mexico	3		Medium	Medium
Morocco	2		Medium	Medium
Netherlands*	3	Yes	High	High
New Zealand*	1	Yes	High	High
Nigeria+	3	Yes	Medium	Medium
Norway*	3		High	High
Oman	1		Low	Medium
Pakistan	4	Yes	Medium	Medium
Panama*	1		High	High
Peru*	2		High	Medium
Philippines	3		Medium	Medium
Poland*	4	Yes	High	High
Portugal*	2		High	High
Qatar	1		High	High

Romania*	2		High	High
Russia+	5	Yes	Low	Medium
Saudi Arabia+	3	Yes	Low	Low
Serbia*	2		High	High
Singapore	3	Yes	Medium	Medium
Slovenia*	1		High	High
South Africa+*	3	Yes	High	High
South Korea*	4	Yes	High	High
Spain*	3		High	High
Sweden*	3	Yes	High	High
Switzerland*	3		High	High
Syria+	3	Yes	Low	Low
Thailand	3		Medium	Medium
Tunisia	2		Medium	Medium
Turkey+	4	Yes	Medium	Medium
Ukraine	3		Medium	Medium
United Arab Emirates	3		Low	Low
United Kingdom+*	5	Yes	High	High
United States+*	5	Yes	High	High
Uruguay*	3		High	High
Uzbekistan	2		Low	Low
Venezuela	2		Medium	Medium
Vietnam	3		Low	Medium

REFERENCES

[1] Forrest Hare, 'The Significance of Attribution to Cyberspace Coercion: A Political Perspective' 4th International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2012), 131.

[2] Dmitri Alperovitch, 'Towards Establishment of Cyberspace Deterrence Strategy' 3rd International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2011), 91.

[3] Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Colorado Springs, CO: U.S. Air Force Academy, 1999), 17.

[4] Gregory Rattray and Jason Healey, 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use' Proceedings of a Workshop on Deterring Cyberattacks (Washington, DC: National Academies Press, 2010), 88.

[5] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton & Company, 2011), 50.

[6] Barry Buzan, *People, States, & Fear: An Agenda for International Security Studies in the Post-Cold War Era* (London, UK: ECPR Press, 1991), 134.

[7] Forrest Hare, 'The Cyber Threat to National Security: Why Can't We Agree?' 2nd International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2010), 218.

[8] Ibid.

[9] Melissa Hathaway, 'Developing International Norms for a Safe, Stable, and Predictable Cyber Environment' Georgetown University Conference on International Engagement on Cyber, March 4, 2014.

[10] Jason Rivera, 'North Korea Has Crossed the Cyber Red Line by Combining Cyberattacks with the Threat of Terrorism—and the United States Must Respond' (2014) *Georgetown Security Studies Review* http://georgetownsecuritystudiesreview.org/2014/12/18/north-korea-has-crossed-the-cyber-red-line-by-combining-cyberattacks-with-the-threat-of-terrorism-and-the-united-states-must-respond/ (accessed 19 Dec. 2014).
[11] British Columbia, 'Security News Digest' http://www.cio.gov.bc.ca/local/cio/informationsecurity/pdf_securitynewsdigest/02_24_2015.pdf (accessed 16 Mar. 2015).
[12] Ibid.
[13] RBN Exploit 'Russian Business Network (RBN)' HostExploit, 2014. http://rbnexploit.blogspot.com/ (accessed 4 Nov. 2014).
[14] Brian Krebs, 'Home Depot Hit by Same Malware as Target' krebsonsecurity.com, 2014. http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ (accessed 4 Nov. 2014).
[15] U.S. Embassy Beijing, 'New PRC Internet Regulations' Federation of American Scientists, 1998. https://www.fas.org/irp/world/china/netreg.htm (accessed 6 Apr. 2014).
[16] Jonathan Zittrain and Benjamin Edelman, 'Empirical Analysis of Internet Filtering in China' Harvard Law School, Berkman Center for Internet and Society, 2003. http://cyber.law.harvard.edu/filtering/china/ (accessed 6 Apr. 2014).
[17] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 27.
[18] W. Earl Boebert, *A Survey of Challenges in Attribution* (National Academies Press Online 2010), 44.
[19] Ibid.
[20] U.S. Senator Sheldon Whitehouse (Rhode Island), Comments made at Georgetown University Conference—International Engagement on Cyber: Developing International Norms for a Safe, Stable, and Predictable Cyber Environment, March 4, 2014.
[21] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Mandiant 2013), 19.
[22] Jason Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks' Atlantic Council, Cyber Statecraft Initiative (Washington, DC: Atlantic Council, 2012), 1.
[23] Ibid.
[24] Ibid., 2.
[25] 'Ten Years After: The FBI Since 9/11,' FBI website, 2014. http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/cyber (accessed 19 Apr. 2014).
[26] Jaikumar Vijayan, 'US Tops List of Countries Hosting Malware and Botnets' securityintelligence.com, 2014. http://securityintelligence.com/news/us-tops-list-of-countries-hosting-malware-and-botnets/#.VQa82PnF-So (accessed 16 Mar. 2015).
[27] U.S. House Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, 'Iranian Cyber Threat to the U.S. Homeland' April 26, 2012. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm (accessed 19 Apr. 2014).
[28] DHS Office of Cybersecurity & Communications, 'Cyber News Spotlight: Insight on Cybersecurity News & Trends for Critical Infrastructure' http://www.htcia.org/wp-content/uploads/Cyber-News-Spotlight-February-2014.pdf (accessed 16 Mar. 2015).
[29] Andreas Hagen, 'The Russo-Georgian War 2008' in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 197.
[30] Dorothy Denning, 'Stuxnet: What Has Changed?' (2012) 4 *Future Internet*, 673.
[31] Joshua Kopstein, 'Stuxnet Virus Was Planted by Israeli Agents Using USB Sticks, According to New Report' *The Verge*, 2012. http://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran (accessed 19 Apr. 2014).
[32] Jonathan Diamond, 'Early Patriotic Hacking,' in Jason Healey (ed.) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 138-139.
[33] 'Significant Cyberattack Incidents: Operation Orchard, 2007' Real Clear Politics, 2013. http://www.realclearpolitics.com/lists/cyber_attacks/op_orchard.html (accessed 16 Apr. 2014).
[34] Ibid., 21.
[35] Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks', 4.
[36] Michael Schmitt et al., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press 2013), 45.
[37] UN Charter, art. 2, para. 7.
[38] Ibid., 46.
[39] International Court of Justice, 'Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*, 1986)' www.icj-cij.org. http://www.icj-cij.org/docket/index.php?sum=367&p1=3&p2=3&case=70&p3=5 (accessed 22 Apr. 2014).

[40] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 48-49.
[41] Patricia Figliola et al., 'U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology' Congressional Research Service (Washington, DC: GPO 2011), 10.
[42] Jason Rivera, 'Understanding and Countering Nation-State Use of Protracted Unconventional Warfare' (2014) *Small Wars Journal* http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare (accessed 24 Dec. 2014).
[43] 18 U.S.C. § 1030: US Code—Section 1030: Fraud and related activity in connection with computers.
[44] Jason Rivera and Forrest Hare 'The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures' 6th International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications 2014), 109-110.
[45] Andru Wall, 'Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action' *Harvard National Security Journal* 3 (2012), 118.
[46] Rivera & Hare, 'The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures', 112.
[47] Ibid., 113.
[48] Global Fire Power, 'Countries Ranked by Military Strength,' www.globalfirepower.com, 2014. http://www.globalfirepower.com/countries-listing.asp (accessed 9 May 2014).
[49] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, Inc., 2011), 243-261.
[50] Arch Puddington, *Freedom in the World 2014* (Washington, DC: Freedom House 2014), 18-22.
[51] Ibid.