GLOBAL RELATIONS FORUM YOUNG ACADEMICS PROGRAM
POLICY PAPER SERIES No.5

STATE RESPONSES TO CYBER OPERATIONS

DR. FRANÇOIS DELERUE

European University Institute, Ph.D. in Law

GİFGRF

Global İlişkiler Forumu Global Relations Forum

GLOBAL RELATIONS FORUM YOUNG ACADEMICS PROGRAM POLICY PAPER SERIES No.5

STATE RESPONSES TO CYBER OPERATIONS

Dr. François Delerue

European University Institute, Ph.D. in Law

Global Relations Forum Young Academics Program
Policy Paper Series No.5

State Responses to Cyber Operations
by Dr. François Delerue

July 2017

ISBN: 978-605-83113-2-9

Publisher Certificate No: 22780

Printed in Turkey
Gren Agency, Istanbul. www.grenajans.com

Please direct inquiries to:

GLOBAL RELATIONS FORUM
Yapı Kredi Plaza D Blok Levent 34330
Istanbul, Turkey
T: +90 212 339 71 51 F: +90 212 339 61 04
www.gif.org.tr | *info@gif.org.tr*

This publication can be downloaded at gif.org.tr

Contents

About GRF

Global Relations Forum (GRF), founded in 2009 with the support of prominent Turkish leaders in business, government and academia, is an independent, nonprofit membership association committed to being a platform for engaging, informing, and stimulating its members and all interested individuals in all matters related to international affairs and global issues.

GRF intends to advance a culture that rewards the fertile tension between passion for intellectual diversity and dedication to innovative and objective synthesis. It nurtures uninhibited curiosity, analytic inquiry, rational debate, and constructive demeanor as the elemental constituents in all its endeavors. It contributes to the shared understanding of and aspiration for humanity's path to peace, prosperity, and progress as an accessible, inclusive, and fair process for all.

About the GRF Young Academics Program

Global Relations Forum community programs aim to advance a culture of intellectual diversity, rational and constructive debate, and analytic coherence.

GRF Young Academics Program is distinct among these community initiatives as it serves an additional but equally important objective. Through this program, GRF is establishing an expanding network of young academics that contributes to policy discussions both in international and national spheres.

The program is designed to culminate in the publication of either a policy or an analysis paper authored by the young academic, which is then published as part of the Policy Paper Series or the Analysis Paper Series. The author benefits from the experience of GRF members in crafting her paper. However, the publication reflects the views of the young academic and not the institutional views of GRF or the individual positions of the commission members.

This paper entitled *"State Responses to Cyber Operations"* is authored by Dr. François Delerue as part of the *GRF Young Academics Program Policy Paper Series*. GRF thanks him for his contribution and commitment to this effort.

GRF convened the following group of distinguished members to evaluate and guide Dr. François Delerue's paper:

Memduh Karakullukçu
Vice Chairman and President of GRF

Mustafa Özbey
Admiral (R); Board Member, Erciyas Steel Pipe Co.

Ümit Pamir
Ambassador (R); Former Permanent Representative of Turkey to the United Nations

Cengiz Ultav
Chairman of the Board of Directors, Technology Development Foundation of Turkey; Executive Board Member, Vestel Ventures

GRF is grateful to all members who participated in the evaluation commission for their invaluable insights, informed guidance as well as for the time and effort they dedicated to the program.

Global Relations Forum

About the Author

Dr. François Delerue is a researcher in cyber defense and international law at the French Institute of Strategic Studies of the Military School (*Institut de Recherche Stratégique de l'École Militaire* - IRSEM), an associate researcher at the Castex Chair of Cyber Strategy and a visiting researcher at the Sciences Po Law School in Paris. He is also a rapporteur for the Oxford International Organizations project. He was a consultant in cybersecurity and cyberstrategy at CEIS *(Compagnie Européenne d'Intelligence Stratégique)*, a consultancy firm in Paris. He defended his Ph.D. on cyber operations and international law in November 2016 at the European University Institute (EUI – Florence, Italy) under the supervision of Professor Nehla Bhuta. His research was sponsored by the French Institute of Higher National Defense Studies *(Institut des Hautes Études de Défense Nationale* – IHEDN), IRSEM and the French Ministry of Research. He taught at the International Institute for Humanitarian Law at Sanremo, the Portuguese National Defense Institute (IDN), the University of Florence, and the EUI. He was a visiting researcher at Columbia University in New York (2014), and attended the 62nd youth seminar of the IHEDN (2009) and the international law and cyber operations seminar of the NATO School in Oberammergau (2013.)

Global Relations Forum Young Academics Program
Policy Paper Series No. 5

State Responses to Cyber Operations

Dr. François Delerue

European University Institute, Ph.D. in Law

francois.delerue@eui.eu

Abstract

This policy paper describes the range of possible classifications of state-sponsored cyber operations and the lawful responses that states targeted by them can take. Based on this assessment, the paper recommends that these findings be integrated into national cyberstrategies that can more effectively counter state-sponsored cyberthreats and operations.

• Most state-conducted or state-sponsored cyber operations do not qualify as a use of force and, *a fortiori*, an armed attack;

• Most state-sponsored cyber operations neither occur during an ongoing armed conflict nor constitute a new armed conflict;

• In most situations, a state targeted by state-sponsored cyber operations is not entitled to invoke the right of self-defense to use force against the attacking state, and thus the victim state's response must be peaceful;

• In most situations, the international law of countermeasures is the most appropriate framework to determine which responses are available to the victim state;

• The attribution of state-sponsored cyber operations remains difficult, but states should still define and expand their cyber policies so that they can adequately respond to such operations.

1. Introduction

The digital revolution has transformed human societies. The Internet, and more generally computer networks, have become ubiquitous and indispensable for humankind to function, affecting every aspect of modern life. Several significant threats and obstacles, however, challenge the functionality of the Internet and the powerful opportunities that it offers. To start, unequal access to computers and computer networks as well as government censorship limit Internet access. More alarmingly, computer networks can be used for malicious activities that threaten national and international security. Every day, media reports describe cyber operations that target and sometimes seriously hurt individuals, companies, and states. As a result, cybersecurity has become a key issue for global security. Numerous actors now view this new reality as an opportunity to carry out malicious activities that either mimic previous ones or are wholly original. These activities are categorized according to their perpetrators. Cybercrime and cyberterrorism involve non-state actors, while state-sponsored cyber operations are generally labelled cyberwarfare. Cyber espionage can encompass both state and non-state actors.

Academic and political debates in the field of cybersecurity mainly focus on cyberthreats perpetrated by non-state actors, such as individuals, groups, companies, or private military and security companies. Non-state actors are both the main perpetrators and the main targets of malicious cyber activities. Yet cyberthreats arising from states or their proxies that target other states should not be neglected. The most harmful and disruptive examples of cyber operations, such as the malware Stuxnet that physically damaged an Iranian nuclear plant or the large-scale distributed denial-of-service (DDoS) attacks against Estonia and Georgia, were, allegedly, state-sponsored.

State-sponsored cyber operations are generally labelled "cyberwarfare," which is defined as the recourse to cyber means by one state against another. This is neither a legal nor a prescriptive term; it reflects, however, a disproportionate focus on the realm of warfare. Avoiding hasty or overly simplistic characterizations of cyber-related situations as cyberwarfare will help prevent unnecessary conflict escalation and assist targeted states in identifying and applying the appropriate response to each kind of cyberthreat.

What is "cyberwarfare"?

State-sponsored cyber operations are generally defined as "cyberwarfare," but this term is oftentimes inaccurate as most operations fall outside of the realm of (cyber) warfare. What, then, is cyberwarfare and what does it imply?

"Cyberwarfare" is constructed from the prefix "cyber," which refers to a relationship with the Internet and computer technology, and "war." In simple terms, it is the waging of war using computer technology and the Internet. The term "war," or "warfare," can be defined as an armed conflict between states or non-state actors to impose a determined will by force. The occurrence of an armed conflict leads to a change in the applicable law: some rules that are valid in peacetime are no longer applicable in war, and the law of armed conflict applies instead. After the Second World War, the term "war" was deemphasized in international law and other

terms – such as armed conflict and use of force – replaced it. Cyberwarfare is a coin with two misleading sides. On the one hand, it implies that cyber operations amount to or take place during an armed conflict and thus the law of armed conflict is applicable to them. On the other hand, it implies that cyber operations violate the prohibition against the use of force in international law. Since these two situations only occur in a small portion of state-sponsored cyber operations, it is misleading to refer to state-sponsored cyber operations as cyberwarfare.

Yet cyber operations can occur either during an existing armed conflict, as during the Russo-Georgian conflict in 2008, or can themselves constitute a new armed conflict, although there is no such example to this date. The vast majority of cyber operations neither occur during an existing armed conflict nor constitute a new armed conflict as such. Consequently, this policy paper focuses on cyber operations that occur during times of peace. This allows us to analyze the legal regime applicable to cyber operations, and how victim states can respond to them.

It is important to recall that there are a number of possible classifications of state-sponsored cyber operations that fall outside the realm of cyberwarfare. Most state-sponsored cyber operations do not, in fact, violate the prohibition of the use of force or the law of armed conflict; rather, they violate the territorial sovereignty of the targeted state or the principle of non-intervention. Cyberwarfare is also only the tip of the iceberg, as an entire world of cyber operations below the threshold of cyberwarfare lies submerged. Consequently, it is important not to use the term cyberwarfare in a prescriptive manner based on the narrow understanding of cyber operations it implies. Such an approach risks classifying most state-sponsored cyber operations inaccurately by omitting to consider alternatives.

This policy paper describes the wide range of possible classifications of state-sponsored cyber operations and explains the different countermeasures that victim states can take. The important output of this paper is to present various lawful responses to state-sponsored cyber operations.

This policy paper also highlights the necessity of integrating these classifications and their possible responses into national cyberstrategies. Indeed, nations have adopted strategies to cope with cyber operations in two distinct phases. In the first phase, they dealt with the pressing situation of growing cyberthreats and tried to integrate solutions that went beyond simple cyber responses. The urgency of the situation led states to focus on devising more robust military and self-defense strategies. In the second phase that is currently underway, states will need to integrate the wide range of possible classifications of state-sponsored cyber operations into their national strategies. In the process, states can develop responses that are appropriate and effective for all types of cyberthreats.

Selected examples of alleged state-sponsored cyber operations

2007 - Estonia

On April 26-27, 2007, Estonia experienced violent street protests in the center of its capital Tallinn, mainly by a minority group of Russian descent, after it decided to remove and relocate a bronze war memorial of a Soviet soldier commemorating Russia's victory in the Second World War. The riots were accompanied by cyber operations that began on April 27 and continued for nearly three weeks until May 18.

As the cyber attacks were emanating from numerous countries around the world, the Estonian government could not identify the perpetrators. It accused Russia of orchestrating the attacks, but lacked evidence to support its claim.

Estonia initially explored the possibility of invoking Article 5 of the North Atlantic Treaty, thus treating the cyber operations as an "armed attack," triggering the "right of individual or collective self-defense."[1] This solution was, however, quickly ruled out.

2008 - Georgia

After Georgia launched a large-scale military offensive in South Ossetia against separatist provocations, an armed conflict erupted between Russia and Georgia from August 7 to 12, 2008.

Cyber operations targeting Georgia allegedly started on August 8, just before the Russian invasion, and lasted until the end of the month.[2] The International Fact-Finding Commission on the Conflict in Georgia, which was established by the Council of the European Union to investigate the origins and the course of the conflict, dedicated part of its report to detailing the scope of these cyber operations without giving them legal qualification under international law.[3]

Cyber operations mainly took the form of website defacements and DDoS attacks. There were also significant levels of e-mail spamming. The targets were the Georgian government and media, as well as some commercial and private actors. Instructions and software to ping flood Georgian websites were available via mainly Russian-speaking blogs, forums and websites. The cyber operations could not be conclusively attributed to a state; the DDoS attacks were identified as coming from many different countries.

2010 - Stuxnet

Stuxnet was a computer worm that infected and disrupted Iranian nuclear facilities in 2007, resulting in the physical destruction of several centrifuges. The worm also infected numerous computers around the world.

---

[1] North Atlantic Treaty, Article 5: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

[2] See the study in: Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations" (NATO Cooperative Cyber Defence Centre of Excellence, 2010), 68–90, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[3] Report of the International Fact-Finding Commission on the Conflict in Georgia, September 2009, Vol. II, 217-219, http://www.ceiig.ch/Report.html

The Belarusian security company VirusBlokAda initially identified Stuxnet in June 2010. Many alleged that it was designed and launched by the United States and Israel, perhaps with the help of other countries, in order to coerce Iran to modify its nuclear program and abandon its military nuclear ambitions.

2014 - Sony Hack

In 2014, the computer networks of Sony Pictures Entertainment, the American subsidiary of the Japanese conglomerate Sony Corporation, was hacked, and an important amount of data was stolen from the company and released publicly in November 2014. The hackers notably demanded the cancellation of the release of the film *The Interview*, a comedy about the assassination of North Korean leader Kim Jong-un. US officials alleged that North Korea sponsored the attack, but North Korea denied all involvement.

2016 - DNC Hack

On July 22, 2016, the WikiLeaks website published 19,252 emails and 8,034 attachments stolen from the Democratic National Committee (DNC), the governing body of the Democratic Party in the United States.[4] The leak occurred during the campaign for the 2016 Democratic Party presidential primaries and a few days before the Democratic National Convention. It disrupted the internal voting process and led certain party executives to resign. The party was already aware that it had been hacked a few months before WikiLeaks published the documents and had enlisted the American cybersecurity company Crowdstrike to investigate. In June 2016, Crowdstrike published its conclusions: the hacking was the work of two different groups called Cozy Bear and Fancy Bear, which acted separately yet simultaneously, in the information technology networks of the Democratic Party.[5] These two groups did not limit themselves to the hacking of the Democratic Party; they also targeted the Republican Party (though to a lesser extent) and other institutions including think tanks in the context of the American elections.

On October 7, 2016, the Department of Homeland Security and the Office of the Director of National Intelligence published a joint report affirming that the Russian government was responsible for various hacks and the online publication of Democratic Party documents.[6] On October 10, 2016, the White House announced that the US government would adopt a proportionate response and, on December

---

[4] Karen Tumulty and Tom Hamburger, "WikiLeaks Releases Thousands of Documents about Clinton and Internal Deliberations," Washington Post, July 22, 2016, https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/

[5] Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," Crowdstrike, June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

[6] United States, DHS and FBI, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security | Homeland Security," October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national; Ellen Nakashima, "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections - The Washington Post," Washington Post, October 7, 2016, https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.83a87b1a2451

29, 2016, it launched new sanctions against Russia and certain individuals. President Obama also expelled 35 Russian diplomats from the country, who left US territory on January 1, 2017. Some commentators purport that the United States also used extrajudicial measures, including cyber operations against Russian interests, although these have not been officially acknowledged. In late October 2016, Ukrainian hackers calling themselves Cyber Hunta hacked email accounts associated with Vladislav Surkov, a close advisor to the Russian president, and published emails and documents online. These leaks provided proof of Russian involvement in the separatist movements in eastern Ukraine.[7]

2. Current responses to state-sponsored cyber operations

Most states have adopted national strategies to deal with cyberthreats, notably those arising from other states. The content of these strategies has been generally influenced by two events. Firstly, the public exposure of the mass surveillance programs conducted by the US National Security Agency (NSA) and the UK Government Communication Headquarters (GCHQ), in cooperation with Australia, Canada and New Zealand, shined the spotlight on espionage practices in the cyber age. Today, states are concerned about cyber espionage as a form of state-sponsored cyberthreat.[8]

Secondly, and most importantly, the development of large-scale cyber operations, allegedly conducted by one state against another, led states to explore ways to respond outside of the cyber realm. Large-scale cyber operations that steal data, reveal information, and even produce physical damage to the victim state, have prompted states to consider using kinetic force – e.g. dropping a bomb or launching a military intervention – in retaliation to cyber operations. However, most cyber operations have limited effect, and victim states do not want to publicize the fact that they were attacked. In case of a cyber operation, the victim state will prefer to mitigate the negative effects of the operation or respond through cyber means. Since there is no general prohibition against cyber operations, the victim state will act in a legal grey area.

In this respect, the cyber attacks against Estonia in 2007 were a watershed in shaping the cybersecurity strategies of NATO and Estonia, and raising international awareness about the potential consequences of cyber operations. They led to the creation of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in August 2008. In 2009, the CCDCOE launched the Tallinn Manual Process,

---

[7] Andrew Buncombe, "Russia Hacked: Putin's Aide Has Secrets Spilled by Ukrainian Group, Sparking Suspicions of Proxy Cyberwar," Trump V Clinton, October 28, 2016, http://trumpxclinton.com/widget-horizontal/

[8] It is essential to understand the diversity of cyber operations and to not reduce them to cyber espionage conducted from the territory of the perpetrating state. The latter tend to mislead us in a situation where we cannot see the forest for the trees. Cyber espionage indeed receives most of the public's attention. Cyber espionage conducted on the data transiting on the territory of the perpetrating state does not violate the territorial sovereignty of the targeted state, but this conclusion cannot be extended to all kinds of cyber operations. One notable exception is when states are penetrating ICT infrastructure located on the territory of targeted states

which led to the publication in 2013 of *The Tallinn Manual on the International Law Applicable to Cyberwarfare*.[9] Although not an official NATO or CCDCOE document, the manual was written by a group of international experts and has become influential in determining how to apply international law to state-sponsored cyber operations and states' cyberstrategies.

Though the *Tallinn Manual* provides a comprehensive study of cyberwarfare, it deals with other situations quite superficially. A second edition of the manual was published in February 2017 that seeks to apply international law to cyber operations that are below the threshold of cyberwarfare.

The cyber attacks against Estonia and the *Tallinn Manual* reveal two phases in the evolution of cyberstrategy. The first phase focused on "cyberwarfare" and how to respond to state-sponsored cyber operations through military means. The second phase, illustrated by the new edition of the *Tallinn Manual*, expanded the scope to include other possible characterizations of cyber operations and to detail appropriate responses.

3. Lawfulness of state-sponsored cyber operations

There is no general prohibition against state-sponsored cyber operations, but such operations might violate specific norms of international law, depending on their characteristics and effects. Policymakers have focused on the prohibition of the use of force in international law, and have sought to classify cyber operations as armed attacks that trigger the right of states to self-defense. However, as highlighted in this policy paper, other classifications are possible and, in most cases, more accurate than classifying such operations as armed attacks.

It is important to note that a number of circumstances could preclude cyber operations from being rendered unlawful. This is the case if they are conducted under situations of distress, necessity, or as the result of *force majeure*.[10] These situations are quite specific and do not apply to most cyber operations; consequently, they are not discussed here.

3.1 No general prohibition

In many respects, state-sponsored cyber operations are comparable to state-sponsored espionage; no general prohibition exists under international law, as each state is willing to preserve its own capacity to conduct such operations.[11]

---

[9] Michael N. Schmitt, ed., The Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013)

[10] See generally on the circumstances precluding wrongfulness: James Crawford, Alain Pellet, and Simon Olleson (ed.), The Law of International Responsibility (Oxford University Press, 2010), chapters 32 and 33, 427-502; James Crawford, State Responsibility: The General Part (Cambridge University Press, 2013), 274-324

[11] Fabien Lafouasse, L'espionnage Dans Le Droit International, Collection Le Grand Jeu (Paris: Nouveau monde, 2012), 25 et seq.; Fabien Lafouasse, "L'espionnage En Droit International," Annuaire Français de Droit International 47, no. 1 (2001): 63–136; Christian Schaller, "Spies," MPEPIL, April 2009; Roger D. Scott, "Territorially Intrusive Intelligence Collection and International Law," Air Force Law Review 46 (1999): 217–18

States do not want to impose legal limits on their capacity to act in this grey area and recognize the difficulty of determining whether a cyber operation was launched with hostile intent.

Yet cyber operations could constitute inimical or unfriendly acts. An unfriendly act can be defined as a state's conduct (act or omission) that, without being contrary to international law, inflicts disadvantage, disregard, or discourtesy on another state and is thus considered by the latter as a breach of good relations. This renders their relationship more complicated, but does not bring legal consequences.

Unfriendly acts are lawful; they do not invoke the right of states to conduct unlawful acts as countermeasures or self-defense. The victim state of an unfriendly act can, however, take measures of retorsion – i.e. another unfriendly act.

3.2 Threat or use of force

The prohibition against the threat or the use of force is enshrined in Article 2, Paragraph 4 of the United Nations Charter, and is universally accepted as a norm of customary international law. States are prohibited from using force against each other. Yet the prohibition does not include all types of force; for instance, economic, political or indirect forces are excluded.

Are states prohibited from using cyber force? Cyber operations clearly fall under the prohibition against the use of force, but not all forms of cyber operations amount to a use of force, and thus, not all cyber operations are prohibited. The consequence-based test is generally used to determine whether a cyber operation violates the prohibition against the use of force. The consequence-based approach focuses on the outcomes of cyber operations (virtual consequence, physical destruction, or death); cyber operations that cause physical destruction or death would always qualify as use of force, whereas operations that have non-physical consequences are more controversial.

In a nutshell, a cyber operation must meet two criteria in order to violate the prohibition against the use of force:

- being state-sponsored, as only states are bound by this prohibition;
- being of a certain intensity (generally, resulting in physical destruction or death.)

Stuxnet infected and disrupted the Iranian nuclear program in 2007, physically destroying several centrifuges. It is generally considered the only cyber operation that potentially violated the prohibition of the use of force.

3.3 Armed attack

Article 51 of the United Nations Charter asserts that a state needs to be the victim of an armed attack in order to exercise its right of self-defense. Armed attacks are the "most grave forms of the use of force," according to the International Court of Justice.[12]

---

[12] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), (Merits), I.C.J. Reports 14 (1986), 101, para. 191

However, some commentators challenge this interpretation and suggest that the notions of armed attack and use of force are equivalent, which would mean that all use of force triggers a state's right of self-defense. The distinction between an armed attack and the use of force seeks to avoid disproportionate military action in response to minor incidents, such as border clashes, but this distinction is not clearly agreed upon.

The vast majority of cyber operations do not qualify as use of force and, *a fortiori*, cannot be considered as armed attacks. Accordingly, they do not trigger the right of self-defense. Cyber operations that inflict significant damage and loss of life, such as causing an aircraft to crash or a dam to open, will most likely be considered an armed attack. To date, no cyber operation has seriously been considered an armed attack.

3.4 Territorial sovereignty

Territorial sovereignty grants states the right to exercise full and exclusive authority over their land territory and its appurtenances, including internal waters, territorial sea, archipelagic waters, airspace, and subsoil. Any unauthorized state-sponsored cyber operation penetrating a foreign computer system constitutes a violation of territorial sovereignty of the victim state.

Two conditions must be met for a cyber operation to violate the territorial sovereignty of a state:

- being attributable to a state;
- penetrating the computer system of the victim state.

There is no required level of damage to deem a cyber operation a violation of a state's territorial sovereignty. Any state-sponsored cyber operation that penetrates or affects a foreign computer system that is attributable to a state would violate it. Yet some experts, notably within the international group of experts who authored the *Tallinn Manual*, express doubt that this definition can be applied to cyber operations and argue that damage is a necessary component:

> A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage. The international group of experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty.[13]

An example from outside the cyber realm reveals how damage is not necessary to confirm that sovereignty has been violated. The mere trespassing of airplanes or ships, for instance, constitutes a violation of territorial sovereignty without any damage requirement.

Denial-of-service (DoS) attacks do not involve the planting of malware into the targeted computers. There is, therefore, no penetration into a foreign system, but they still negatively affect it. For a majority of scholars, the occurrence of the effects within a foreign system suffices to constitute a violation of territorial sovereignty. Consequently, a state-sponsored DoS attack in a foreign state might be considered a violation of territorial sovereignty.

---

[13] Schmitt, The Tallinn Manual, 16, para 6, commentary under Rule 1

3.5 Principle of non-intervention or non-interference

The principle of non-intervention prohibits the interference by a state in the internal or foreign affairs of another state. Three elements constitute an unlawful intervention:

- being carried out by a state acting against another state. An act carried out by a private individual or group could also qualify, if it is attributable to a state;
- affecting matters in which the victim state is permitted to decide freely, either external or internal affairs;
- being an attempt to coerce the victim state by directly or indirectly interfering in its internal or external affairs.

An unlawful intervention might take a variety of forms, including the use of force, subversive intervention, diplomatic intervention, political interference, extraterritorial enforcement jurisdiction or economic coercion. An intervention carried out by the use of force would violate both the principle of non-intervention and the prohibition of the use of force.

Many believe that Stuxnet was aimed at coercing Iran into modifying its nuclear program and renouncing its military nuclear ambitions. If state sponsorship of Stuxnet could be proved, it would constitute an unlawful intervention.

The 2014 hack of Sony Pictures Entertainment was another interesting example. In a statement released in December 2014, then US Secretary of Homeland Security Jeh Johnson declared that "[t]he cyber attack against Sony Pictures Entertainment was not just an attack against a company and its employees. It was also an attack on our freedom of expression and way of life."[14] One could see this statement as criticizing the intervention within the context of the internal affairs of the United States. Does the hack of Sony Pictures Entertainment and the resulting situation constitute a violation of the principle of non-intervention? The attribution of this hack to North Korea is still not clear. Moreover, the attack clearly targeted a private actor and not the United States, and thus it cannot be considered an unlawful intervention.

[14] "Statement by Secretary Johnson On Cyber Attack On Sony Pictures Entertainment," US Homeland Security, December 19, 2014, http://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment

4. Potential responses

This section highlights the different potential responses to state-sponsored cyber operations. It must be noted that in addition to responding, the victim state is also empowered to ask the responsible state for reparations in the form of restitution, compensation, or satisfaction.

4.1 Self-defense

The customary right to self-defense enshrined in Article 51 of the United Nations Charter is the principle exception to the prohibition against the use of force. A state targeted by a cyber operation constituting an armed attack has the right to resort to self-defense, using either cyber operations or other forms of force such as kinetic force. The right of self-defense requires that three conditions be met:

- being in response to an armed attack;
- being necessary and proportionate;
- being reported to the UN Security Council. A state must cease its resort to self-defense when the Security Council has taken "measures necessary to maintain international peace and security" (Article 51.)

The right of self-defense is the only circumstance under which a victim state is authorized by international law to use force, including kinetic force such as launching bombs, against cyber operations.

The victim state can act in self-defense either alone or in conjunction with other states in collective self-defense. In the case of collective self-defense, at least one of the states must be the victim of an armed attack and must declare that it is the victim of an armed attack. Moreover, the assistance of other states must have been requested by the victim state.

The vast majority of cyber operations do not qualify as a use of force and, *a fortiori*, an armed attack. Consequently, in such cases, the victim state does not have a right to self-defense and thus cannot recourse to kinetic force.

4.2 Security Council of the United Nations

The recourse to force against cyber operations may be authorized by the Security Council of the United Nations under Chapter VII of the United Nations Charter. The Security Council might indeed designate a specific cyber operation as a "threat to the peace, breach of the peace, or act of aggression" (Article 39) and can thus make recommendations (Article 40) or take measures that can involve armed force (Articles 41 and 42.)

4.3 Countermeasures

The victim state of an internationally wrongful act – e.g. a cyber operation that violates the rights of the victim state under international law – may take countermeasures against the responsible state. These countermeasures would normally be unlawful, but their unlawfulness is precluded by the unlawfulness of the first act.

For instance, the victim state of an unlawful state-sponsored cyber operation can respond by launching a cyber operation against the responsible state. The unlawfulness of this cyber operation taken in response to the initial operation will be precluded, as it constitutes a countermeasure.

There are several criteria to constitute a countermeasure:

- being taken in response to an unlawful act by the responsible state;
- being taken after asking the responsible state to cease its act;
- being notified by the reacting state prior to launching countermeasures, unless the countermeasures are urgent;
- being proportionate;
- being terminated as soon as the violation of international law – e.g. the first cyber attack – has ceased.

Most state-sponsored cyber operations are unlawful under international law. If taken as a countermeasure, their unlawfulness could be precluded. Outside of the cyber realm, countermeasures can, for instance, include economic coercion.

4.4 Retorsion

Measures of retorsion are acts that are not unlawful. They are generally unfriendly acts taken in response to a prior unfriendly act.

The lawfulness of certain kinds of cyber operations might still be debatable, and thus they could be considered as not breaching the rights of the victim state guaranteed under international law. Under such circumstances, international law does not allow the victim state to take unlawful measures against the responsible state.

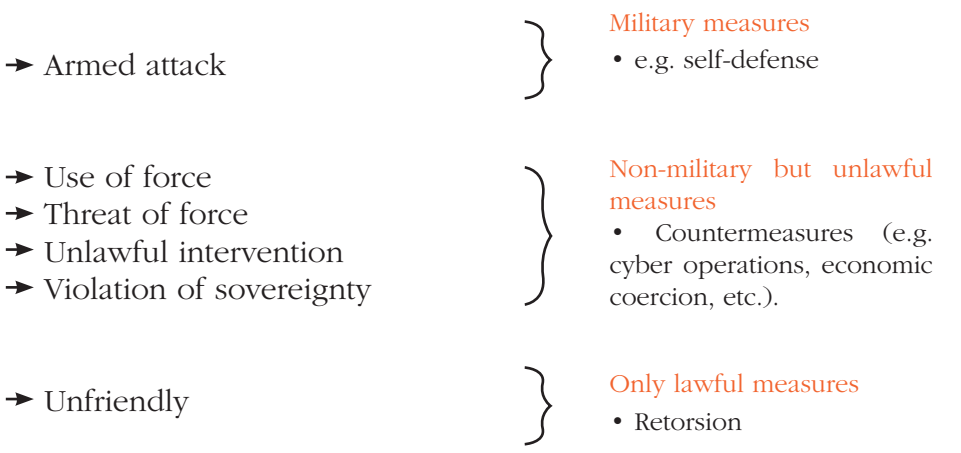
5. Conclusion

This policy paper highlighted the many possible forms of state-sponsored cyber operations as well as lawful measures that might be taken in response. It demonstrates the necessity for states to integrate into their cyber policies the entire spectrum of available responses to different forms of cyber attacks so that they can take the most appropriate measures.

In most cases, state-sponsored cyber operations violate international law but do not amount to an armed attack. Consequently, the victim state cannot recourse to military measures in response, but can recourse to countermeasures such as unlawful cyber operations or economic coercion.

It must be underscored that this paper focused first and foremost on state-sponsored cyber operations. This matter necessitates in turn that the question of attribution be addressed. Indeed, this paper and its arguments are applicable to cyber operations attributed to a state, either because it conducted the operation or because the operation was conducted on its behalf. This paper does not, however, examine the challenges and intricacies of attribution of cyber operations.

Possible responses:



References

Alperovitch, Dmitri. "Bears in the Midst: Intrusion into the Democratic National Committee »," Crowdstrike." Crowdstrike. June 15, 2016. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Buncombe, Andrew. "Russia Hacked: Putin's Aide Has Secrets Spilled by Ukrainian Group, Sparking Suspicions of Proxy Cyberwar." Independent, October 28, 2016. http://www.independent.co.uk/news/world/europe/vladimir-putins-aide-gets-hacked-sparking-suspicions-of-proxy-cyberwar-ukraine-cyberhunta-a7385306.html

Department of Homeland Security and FBI. "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security." News release, October 7, 2016. Department of Homeland Security. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

Lafouasse, Fabien. L'espionnage dans le droit international. Paris: Nouveau Monde, 2012

Lafouasse, Fabien. "L'espionnage en droit international." Annuaire Français de Droit International 47, no. 1 (2001): 63-136. doi:10.3406/afdi.2001.3655

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 14 I.C.J. Reports 101 (International Court of Justice 1986)

Nakashima, Ellen. "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections." The Washington Post, October 7, 2016. https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.73736ad727d5

"North Atlantic Treaty, Article 5." http://www.nato.int/cps/en/natohq/57772.htm

"Report of the International Fact-Finding Commission on the Conflict in Georgia." II (September 2009): 217-19. http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf

Schaller, Christian. "Spies". MPEPIL 2009

Schmitt, Michael N. Tallinn manual on the international law applicable to cyberwarfare: prepared by the International group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013

Scott, Roger D. "Territorially Intrusive Intelligence Collection and International Law." Air Force Law Review 46 (1999): 217-18

Tikk, Eneken, Kadri Kaska, and Liis Vihul. "International Cyber Incidents: Legal Considerations." NATO Cooperative

Cyber Defence Centre of Excellence, 2010, 68-90. https://ccdcoe.org/publications/books/legalconsiderations.pdf

Tumulty, Karen, and Tom Hamburger. "WikiLeaks Releases Thousands of Documents about Clinton and Internal Deliberations." The Washington Post, July 22, 2016. https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.56fbd027f55c

US Homeland Security. "Statement By Secretary Johnson On Cyber Attack On Sony Pictures Entertainment." News release, December 19, 2014. Department of Homeland Security. http://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment

GRF Young Academics Program Publications

The *GRF Young Academics Program Publications* consist of policy and analysis paper series written by the participants of the Young Academics Program. While both series are concerned with thoroughly analyzing a topic of interest, policy papers additionally propose policy recommendations.

The Young Academics Program and its publications are directed by Burcu Baran Türem, GRF Director of Policy Communities.

GRF Program Director Selin Uğurtaş is the editor of the series.

For further information, please contact GRF at info@gif.org.tr.

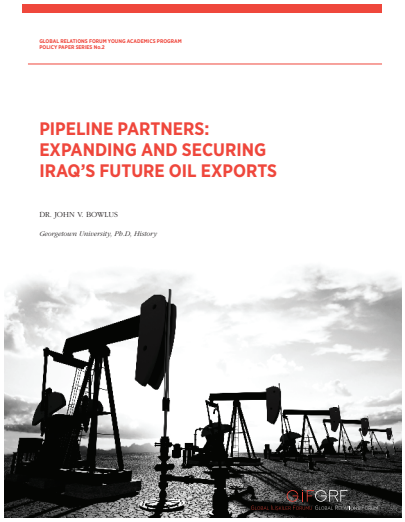
Following is a list of papers published under the *GRF Young Academics Program Publications*.

Policy Paper Series

No: 1

"Turkey in the Eurasian Energy Game" by Onur Çobanlı

Humboldt-Universität zu Berlin, Ph.D. in Economics and Management Science



No: 2

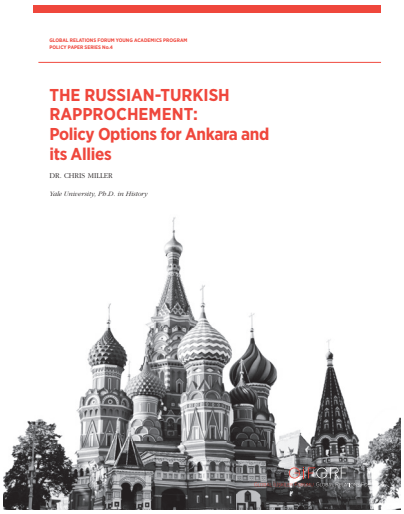
"Pipeline Partners: Expanding and Securing Iraq's Future Oil Exports" by Dr. John V. Bowlus

Georgetown University, Ph.D. in History

No: 3

"Turkey's Foreign Policy Towards China Analysis and Recommendations for Improvement" by Dr. Altay Atlı

Boğaziçi University, Ph.D. in International Relations and Political Science

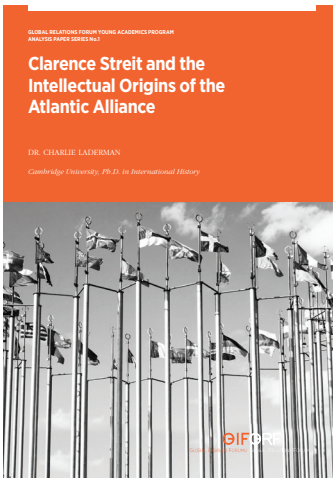


No: 4

"The Russian-Turkish Rapprochement: Policy Options for Ankara and its Allies" by Dr. Chris Miller

Yale University, Ph.D. in History

Analysis Paper Series



No: 1

"Clarence Streit and the Intellectual Origins of the Atlantic Alliance" by Dr. Charlie Laderman

Cambridge University, Ph.D. in International History

All of GRF's publications, including GRF Young Academics Program Publications, can be downloaded from gif.org.tr.

Global Relations Forum Young Academics Program
Policy Paper Series No.5

State Responses to Cyber Operations by Dr. François Delerue

July 2017

GİFGRF

Global İlişkiler Forumu Global Relations Forum

The GRF Young Academics Program brings together young academics who are currently pursuing or have recently completed their doctoral studies. The goal of this program is to provide a forum for accomplished young academics to discuss and define long-term policy challenges.

The GRF Young Academics Program Publications consist of policy and analysis paper series written by the GRF's Young Academics.

Through this program, GRF is establishing an expanding network of young academics to enrich policy discussions both in international and national spheres.

For more information about the Global Relations Forum and the GRF Young Academics Program, you can visit:

www. gif.org.tr

Dr. François Delerue is a researcher in cyber defense and international law at the French Institute of Strategic Studies of the Military School (Institut de Recherche Stratégique de l'École Militaire - IRSEM), an associate researcher at the Castex Chair of Cyber Strategy and a visiting researcher at the Sciences Po Law School in Paris. He is also a rapporteur for the Oxford International Organizations project. He was a consultant in cybersecurity and cyberstrategy at CEIS (Compagnie Européenne d'Intelligence Stratégique), a consultancy firm in Paris. He defended his PhD on cyber operations and international law in November 2016 at the European University Institute (EUI – Florence, Italy) under the supervision of Professor Nehla Bhuta. His research was sponsored by the French Institute of Higher National Defense Studies (Institut des Hautes Études de Défense Nationale – IHEDN), IRSEM and the French Ministry of Research. He taught at the International Institute for Humanitarian Law at Sanremo, the Portuguese National Defense Institute (IDN), the University of Florence, and the EUI. He was a visiting researcher at Columbia University in New York (2014), and attended the 62nd youth seminar of the IHEDN (2009) and the international law and cyber operations seminar of the NATO School in Oberammergau (2013.)

Global Relations Forum
Yapı Kredi Plaza D Blok
Levent 34330 Istanbul, Turkey
T: +90 212 339 71 51
F: +90 212 339 61 04
www.gif.org.tr

GiFGRF
GLOBAL İLİŞKİLER FORUMU GLOBAL RELATIONS FORUM