The Ultimate Challenge: Attribution for Cyber Operations

Amanda G. Hill, Major, USAF

Wright Flyer Papers

Please send inquiries or comments to

Editor
The Wright Flyer Papers
Department of Research and Publications (ACSC/DER)
Air Command and Staff College
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426

Tel: (334) 953-3558
Fax: (334) 953-2269

E-mail: acsc.der.researchorgmailbox@us.af.mil

AIR UNIVERSITY

AIR COMMAND AND STAFF COLLEGE

The Ultimate Challenge: Attribution for Cyber Operations

Amanda G. Hill, Major, USAF

Wright Flyer Paper No. 70

Air University Press
Muir S. Fairchild Research Information Center
Maxwell Air Force Base, Alabama

Commandant, Air Command and Staff College
Brigadier General Evan L. Pettus

Director, Air University Press
Lt Col Darin M. Gregg

Project Editor
Dr. Stephanie Havron Rollins

Copy Editor
Carolyn B. Underwood

Illustrator
L. Susan Fair

Print Specialist
Megan N. Hoehn

Distribution
Diane Clark

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://www.facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Accepted by Air University Press February 2018 and published November 2019.

Disclaimer

This Wright Flyer Paper and others in the series are available electronically at the AU Press website: https://www.airuniversity.af.edu/AUPress/Wright-Flyers/

AIR UNIVERSITY PRESS

Contents

Foreword

It is my great pleasure to present another issue of The *Wright Flyer Papers*. Through this series, Air Command and Staff College presents a sampling of exemplary research produced by our residence and distance-learning students. This series has long showcased the kind of visionary thinking that drove the aspirations and activities of the earliest aviation pioneers. This year's selection of essays admirably extends that tradition. As the series title indicates, these papers aim to present cutting-edge, actionable knowledge—research that addresses some of the most complex security and defense challenges facing us today.

Recently, The *Wright Flyer Papers* transitioned to an exclusively electronic publication format. It is our hope that our migration from print editions to an electronic-only format will fire even greater intellectual debate among Airmen and fellow members of the profession of arms as the series reaches a growing global audience. By publishing these papers via the Air University Press website, ACSC hopes not only to reach more readers, but also to support Air Force–wide efforts to conserve resources. In this spirit, we invite you to peruse past and current issues of The *Wright Flyer Papers* at https://www.airuniversity.af.edu/AUPress/Wright-Flyers/.

Thank you for supporting The *Wright Flyer Papers* and our efforts to disseminate outstanding ACSC student research for the benefit of our Air Force and war fighters everywhere. We trust that what follows will stimulate thinking, invite debate, and further encourage today's air, space, and cyber war fighters in their continuing search for innovative and improved ways to defend our nation and way of life.

BRIAN HASTINGS
Colonel, USAF
Commandant

Abstract

The inherent nature of cyberspace has created an opportunity for adversaries to exploit vulnerabilities of victim state's cyberinfrastructures anonymously for a myriad of reasons. States and nonstate actors can use multiple avenues and techniques to route malicious malware with relative ease and safety. Further, states can utilize nonstate actors in their efforts to achieve political goals with the ability to deny involvement in the act. This is due to both the nature of cyberspace, deficiencies in international law, and the limitations of technical attribution. Therefore, this paper explores what factors, under international law, could be considered in holding nation-states or nonstate actors accountable for malicious cyber acts. The problem/solution method is used to review the relevant deficiencies in international law, general problems associated with attribution in the cyber domain, and other variables that could produce a more comprehensive assessment of whether a particular entity should be held accountable for a cyber action. Instituting and utilizing a multi-dimensional approach to attribution can provide the information necessary to determine responsibility for malicious cyber acts and provide victim states the confidence to respond appropriately.

Introduction

The United States defines cyberspace as a "global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] As a domain, it is necessary to operate in and defend the same as the domains of land, sea, air, and space.[2] The employment of cyberspace capabilities is available for both countries with advanced military capabilities and those countries or organizations that are not technologically advanced.[3] Computer and networks used by state and non-state actors to "disrupt, deny, degrade, or destroy" information and infrastructure is the definition of cyber operations.[4] When ascertaining adversaries in situations involving cyberspace, the anonymity that is inherent to this domain provides an avenue for adversaries to commit acts that take advantage of vulnerabilities within the cyber realm without committing an overt act that would otherwise have serious consequences. For example, a state can deny responsibility for exploitation of vulnerabilities even if the victim state can use forensic techniques to ascertain the origin of the act. Denial is possible because of the infrastructure of cyberspace, which allows cyber operators to conduct cyber operations in relative anonymity. Technology allows cyber perpetrators to mask their identity and make identification of the act, actor, and any state sponsor, very difficult.

Because of the nature of cyberspace, attribution, which is "the action of regarding something as being caused by a person or thing," hostile or malicious cyber acts can be difficult to ascertain.[5] According to Rid and Buchanan, there are three common assumptions related to technical attribution.[6] First, attribution is difficult as a result of the "underlying technical architecture and geography of the Internet."[7] Second, a redesign of the Internet would solve the attribution problem.[8] Finally, the issue of accountability does not lie in the analysis of evidence, but rather the discovery of the evidence.[9] The first assumption describes how the nature of cyberspace interferes when attributing acts to a particular actor. The second assumption further illustrates that the inherent nature of the Internet is the reason attribution is an issue. If the infrastructure was modified to negate the ability of actors to act anonymously, then attribution would not necessarily be a problem. However, the process of attribution in cyberspace is "more nuanced, more common, and more political" than these assumptions allow.[10]

Though technology can aid victim states in attributing hostile cyber acts, assessment of other considerations is necessary before achieving any response. Evaluation of the cyber act itself should occur before any action is

taken because of the implications of the victim states responsibilities under international law. *The Law of Armed Conflict (LOAC) Deskbook* provides additional guidance on the categorization of "use of force" and an "armed attack" in terms of the traditional kinetic attacks that have been used in past conflicts.[11] These categories have been extended to include cyberspace operations that meet the threshold of "use of force" and "armed attacks."[12] However, *LOAC* does not adequately define the threshold of a hostile cyber act that meets the level of "use of force" or an "armed attack." To provide additional guidance in this area, a group of scholarly experts convened and produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[13] Though the *Tallinn Manual* succeeded in providing additional considerations and guidance in the assessment of hostile cyber acts, the experts could not always come to a consensus on the criteria necessary to meet a threshold for "use of force" and "armed attack." The deficiency of law in this area creates an issue for victim states' ability to hold perpetrating states and non-state actors accountable for the employment of hostile cyber acts. Therefore, under international law, what factors could be considered in holding nation states or non-state actors accountable for malicious cyber acts?

In determining whether to hold a state or non-state actor accountable for a malicious cyber act, international law should recognize that in addition to technological means, nation states should also consider other factors, such as human factors. This recognition would acknowledge the challenges inherent to cyber technology while explicitly recognizing the relevance of a more comprehensive framework of accountability for holding other nation states or non-state actors responsible for cyber transgressions.

The challenges of attribution inherent in cyberspace and the requirement implicit in international law regarding knowledge of the source of a hostile act before responding to it, and recognition under international law of a multidimensional approach would provide the victim states of cyber acts greater clarity on the standard that the international community accepts in determining an appropriate course of action.

In unclassified sources, researchers have mostly concentrated on the technical aspects of attribution and the technology available to find certain information,[14] such as the machine or network used in a cyber operation. The geographical area in which the cyber operation occurred, or the types of cyber operations used; however, are left largely unexplored, as are other types of information that should be considered legitimate in ascertaining any source's responsibility for a cyber act.

This paper will utilize the problem/solution method to review the relevant deficiencies in international law concerning cyberspace and cyber operations,

general problems associated with attribution in the cyber domain, and other variables that could produce a more comprehensive assessment of whether a particular entity should be held accountable for a cyber act. Interviews with cyber experts, along with data collected from scholarly sources will assist in the establishment of important variables in attribution. These variables will serve as criteria that this paper posits should be recognized under international law as permissible in determining attribution of cyber acts. Further research and future recommendations of study will be addressed.

The organization of this paper is as follows. A background of international law and policy regarding cyber operations will be explored to provide a context in which attribution exists in the cyber domain. A review of the attribution problem regarding state and non-state actors will provide a context for the importance of developing a successful multi-dimensional approach for the field. The paper's analysis will highlight the deficiencies in the law, limitations of attribution, and the assessment of a multi-dimensional approach to attribution. Finally, the paper will conclude with any limitations of the analysis, general issues still prevalent in the area of cyber attribution, and further recommendations for future study.

Background

> *To exercise its right of self-defense against a hostile actor, the United States must attribute the attack to that hostile actor. This ability to detect, and thus attribute, an attack is critical for both the operational response to the attack and in dealing with the diplomatic and legal fallout.*
>
> -Darren C. Huskinsson, May 2007

Principles of the DoD Law of War Manual and Cyber Operations

The United States works with the international community to apply existing international laws and the principles of the law of war to cyber operations.[15] Specific international laws may apply to cyber operations even though the laws were created before cyberspace became a domain.[16] Therefore, terminology as it relates to cyberspace continues to develop.[17] However, there are certain terms that require definitions that relate specifically to cyber operations to understand the context better and threshold required for responses. For example, the term cyberattack has been used to describe "hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of Internet services."[18] When

applying principles of the law of war, these types of cyber activities, though hostile or malicious in nature, do not meet the threshold of an "armed attack" or allow for a state to declare a response in self-defense under international law.[19] Therefore, for the purposes of this paper, the definition for cyberattacks under Joint Publication 3-12 will be used. Joint Publication 3-12 defines cyberattacks as "cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains."[20] Defining cyber acts as cyberattacks versus other activities, such as cyber exploitations, is important because of the distinction made under international law and the threshold required to meet this definition. Though similar, cyber exploitations are acts directed at retrieving information whereas cyberattacks are acts directed at "disrupting or destroying" a physical system.[21]

Effects of cyber operations are an important variable in determining if the principles of the law of war apply. Cyberattacks that create effects similar to a missile or bomb would meet the threshold of an armed attack and the principles under the law of war would apply.[22] Even if the effects of a cyber operation do not reach the level of an armed attack, the activity could still fall under the principles of the law of war under non-forcible means and methods of war, such as information gathering.[23] However, when the cyber operation does not fall within a category under the principles of the law of war, it is still used as a guide.[24]

During peacetime, collecting information through cyber operations is governed by international law.[25] Unauthorized access to systems in an effort to gather information may or may not rise to the level of an attack, but attribution is a critical process to complete to take any action. Generally, attribution of cyber operations is difficult because of the nature of cyberspace and the ability of adversaries to deny responsibility of an act.[26] Even if the act can be attributed to a particular computer or network, a state can deny involvement or knowledge of the incident. Furthermore, through the interconnected nature of cyberspace, a neutral state that was not party to an incident may be implicated in an act because the act was perpetrated through the neutral state's cyber infrastructure.[27] This is an example of where other factors would be helpful in determining attribution and the responsibility of the act. In a case where a "neutral state" was implicated in a cyber act against a victim state, allowing a victim state to take into consideration the political climate and attitude by the "neutral state" toward that victim state would be probative information in determining the perpetrator of the act.

The cyber operations discussed in the DoD *Law of War Manual* pertain to operations that are defined in the context of acts of war. Cyber operations that

constitute a cyberattack are those that meet military objectives and would cause a specific type of harm, such as loss of life, significant injury to civilians, or substantial damage.[28] The DoD *Law of War Manual* does not provide examples of cyber operations that would constitute a cyberattack; however, it does provide examples of cyber operations that would not constitute a cyberattack. Cyber operations that do not meet the threshold of the definition of cyberattack include, but are not limited to: defacing a government webpage, minor disruption of the Internet, or network services, minor communication interference or disruption, and disseminating propaganda.[29]

Attribution and the Law of Armed Conflict

"Cyberattacks are not accompanied by calling cards. Perhaps the single greatest challenge to the application of the *LOAC* to cyber activity is the challenge of attribution."[30] The *LOAC* provides guidance on the use of force necessary to invoke a nation's right to self-defense.[31] A certain level of response to a cyber act is dependent upon meeting the threshold of the "use of force" under *LOAC*.[32] Cyber activities have been characterized in three ways: (1) cyber activities that fall below the threshold of the state's ability to respond with a use of force; (2) cyber activities that are equivalent to the threshold to respond with a use of force, but do not meet the threshold of an "armed attack;" and (3) cyber activities that are equal to an armed attack.[33] As defined above, cyberattacks that are considered armed attacks must produce consequences equivalent to a physical attack that causes destruction of property, grave injury, and death.[34] "Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right to self-defense."[35]

The issue becomes the characterization of cyber activities that do not meet the threshold of an armed attack.[36] In the application of *LOAC* to the cyber domain and operations, a state may use force directly against a non-state offender if the state is unable or unwilling to address these attacks within its own state as long as *LOAC* is applied.[37] The issue is multidimensional. *LOAC* stipulates certain prerequisites for a state's use of force. Further, the cyber operation has to reach the level of an attack and the damage caused by the attack would have to be assessed first before use of force can be considered.[38] Complicating matters further, certain cyber operations are not clearly connected to the effects those cyber operations may cause.[39]

Another issue is that military targets are difficult to distinguish from civilian cyber targets.[40] Objects that are used for both military and civilian purposes are called "dual-use."[41] For example, a potential dual-use target would

be a cyber operation that used a computer network to open a dam next to a populated area, causing destruction of property and potential loss of life.[42] The use of force in response for situations involving cyber operations may rely more on the consequences of the cyber operation rather than the means in which the cyber operation was carried out.[43]

Once a cyber act has been defined, in the case of *LOAC*, as an armed attack, there must be an analysis of attribution to identify the perpetrator of the act.[44] This step is crucial in determining whether a state can respond with a use of force and exercise its right to self-defense under *LOAC*.[45] Attribution is critical because of the interconnected nature of cyberspace as well. A response in cyberspace can affect and have significant consequences for other neutral parties that the cyber connection may utilize to get to the target.[46] National decision makers must be cognizant of the rules of necessity, distinction, proportionality, and neutrality in assessing an appropriate response in cyber operations under *LOAC*. They must also be able to defend their conclusion of attribution before using force against another state or actor.[47] Before responding, the state must be able to attribute the cyberattack to a particular state or actor in an effort to avoid collateral damage in targeting.

Tallinn Manual on the International Law Applicable to Cyber Warfare

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is a manual that applies international law onto cyber warfare. It is crafted by scholars to provide clarity regarding the ambiguity of international law as it applies to cyber operations.[48] The *Tallinn Manual* provides 95 black letter rules governing cyber acts and includes more defined guidance on the meanings of terms, such as armed attack in the context of cyberspace.[49] It is important to note that the *Tallinn Manual* provides additional guidance and does not constitute international law. Rule 10 states that the "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."[50] The use of force does not necessarily have to be executed by a state's armed forces, but rather it can be carried out by a state's intelligence agencies, by an individual, or by an entity that the state has contracted with and whose conduct could be attributed to the state.[51] In the case of non-state actors, *LOAC*, and therefore Rule 10, does not apply unless the responsibility can be attributed to a state.[52] One of the ongoing issues in determining appropriate, sanctioned action against a state or non-state actor in collusion with a state is that "cyber operations falling below the use of force threshold are more difficult to characterize as a violation."[53]

Rule 11 in the *Tallinn Manual* states that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[54] The United Nations Charter does not provide any criteria on the threshold of the term use of force.[55] According to the team of experts that collaborated on the *Tallinn Manual*, the use of force can utilize an assessment of the scale and effects to determine if the act meets an armed attack.[56] If the scale and effects from a cyber act are similar to those of a traditional kinetic attack, then according to the *Tallinn Manual*, then *LOAC* applies.[57] The *Tallinn Manual* clarifies this assessment even further by making the distinction that merely providing financial means to non-state actors that are employing cyber operations against another state does not constitute a use of force.[58] However, if a state provides the malware and trains the non-state actors to use the malware, then that would meet the threshold of use of force.[59] Sanctuary of non-state actors by a state or a lack of enforcement by a state to stop cyber acts that meet the threshold of use of force is not considered sufficient to attribute the state with a violation of the use of force principle.[60]

The *Tallinn Manual* acknowledged the lack of disparity between the definitions of use of force and armed attack, stating "the distinction between the two concepts is either so narrow as to be insignificant or non-existent."[61] The conclusion of this rule provided that not all cyber acts meet the threshold for use of force. The acts that do meet the threshold of use of force do not have to be directly targeted by the state; however, the *Tallinn Manual* further states that this issue is unresolved because it is unclear from international law what cyber acts short of armed attacks would meet the threshold of use of force.[62] The *Tallinn Manual* provides probable factors that the international community may assess in determining the act's potential for meeting the threshold of use of force.[63] These factors include severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and state responsibility.[64] Though not an exhaustive list, these factors provide a basic understanding as to what a state may consider when determining if the act meets the threshold of use of force.

Furthermore, the *Tallinn Manual* distinguishes the difference in the terms between use of force and armed attack by the United Nations Charter articles that specifically provide rules of law for acts that meet these thresholds.[65] The distinction is important because meeting the threshold of an armed attack can allow the state to respond with force against another state under international law without violating the "prohibition on using force" against that state.[66] If the act does not meet the threshold of an armed attack under international law, then the state cannot lawfully respond with an act that meets the threshold of use of force against the perpetrating state.[67] The ambiguity

between the terms use of force and armed attack can create difficulty for states attempting to assess these acts and respond lawfully.

In terms of defining a cyber act as an armed attack, the *Tallinn Manual* states that "all reasonably foreseeable consequences of the cyber operation" should be considered.[68] For example, if a cyber act targeted a water purification plant, then any illness or death associated with the contamination of water because of that cyber act is foreseeable and would apply to the determination of categorizing the act as an "armed attack."[69] The *Tallinn Manual* concluded that the "lawfulness of the response" to the cyber act would be determined by "the reasonableness" of the state's assessment of an armed attack.[70] Further, it is necessary not only to consider the actor, but also whether that actor is working on behalf of a particular state for the purpose of defining an act as an armed attack.[71] For example, an individual or group of non-state actors conducting cyber operations against a victim state that reaches the scales and effects threshold under the direction of another state would constitute an armed attack.[72] The analysis of whether an individual or group of actors is receiving direction from another state is important because of the controversial nature of defining an act as an armed attack by non-state actors.[73] The United Nations and *LOAC* are "characterized as applicable solely to armed attacks undertaken by one state against another."[74]

The T*allinn Manual* does provide additional considerations on determining an armed attack within the scales and effect threshold. The determination depends on, but is not limited to: "the extent of damage caused by the operation; whether property involved is state or private in character; the status of individuals who have been targeted; and whether the operations were politically motivated."[75] To exercise a victim state's right to self-defense, there should be a determination that an armed attack occurred and a determination into the identity of the actor.[76] When the cyber act reaches the threshold of an armed attack cannot be attributed to a perpetrating state, the issue of sovereignty must be explored.[77] In these particular cases where there is an absence of consent or authorization from the United Nations, the majority of experts concluded that self-defense against a cyber armed attack was permissible in the territory of the state in which the cyberattack occurred when that state did not have the technological means or expertise to take action or the state was unwilling to take effective action in an effort to repress the cyberattack.[78] However, not all experts agreed, and some believed "using force in self-defense on the territory of a state to which the armed attack is not attributable is impermissible."[79]

Attributing Responsibility to a State

If an act is attributed to a state, the victim state should determine what level of responsibility is held by the state before responding.[80] For example, if a victim state is able to determine the physical location of the originating hostile or malicious cyber operation within a particular state, then the victim state must further determine the extent of the state's knowledge of the act and the state's willingness to allow the actor to continue with the hostile or malicious act without consequence. In this determination, the victim state must consider: the state's ability to detect the act; the ability to enforce the prohibition of the act; the tolerance of the act; the encouragement of the act; the potential direction of the act by the state; and the probability that the state is behind the conduct of the act.[81] The state may also distinguish its allowance of certain cyber operations between specific types of acts.[82] For example, a state may allow certain information collection activities but prohibit any malicious cyber operations that impair other states' systems.

Furthermore, the process of "imputed attribution" is another avenue in which a state can assert that another state is responsible for a cyber operation.[83] Imputed attribution is the concept that a state can be held responsible for an individual or group's actions because the state refuses their duty to prevent their state from being used as "a haven or sanctuary" for those responsible for malicious or hostile cyber operations.[84] A state can be considered responsible through imputed attribution when the state consistently fails to impose measures to stop or prevent the individual or groups conducting the cyber operations against another state.[85] However, "the governing principle of state responsibility under international law has been that the conduct of private actors is not attributable to the state unless the state has directly and explicitly delegated part of its tasks and functions to the private entity."[86] Therefore, the attribution process is crucial to proving whether or not a group or individual non-state actors have perpetrated the cyber activity alone or in collusion with the state.

Attribution and Non-State Actors

Attribution of non-state actors in cyberspace can be a major contention for victim states under international law. The International Law Commission's "Draft Articles on Responsibility of States for Internationally Wrongful Acts" represents that states are responsible for "internationally wrongful acts" perpetuated against victim states.[87] These acts have two distinctions.[88] First, the act has to breach an international obligation and second, the act has to be attributable to a state.[89] If a state commits an act that breaches international law,

the state must immediately stop the act or comply with their legal obligation, in the case of an omission, and "make full reparation of the injured state."[90] Therefore, in the case of cyber acts, if the state breaches its international obligation, it is required to cease the cyber act immediately. Further, in the case of non-state actors acting on behalf of a state—in which the cyber act committed by the non-state actors is attributable to that state— the state must follow the same guidelines. If the perpetrating state does not fulfill its duty under international law, victim states may take countermeasures, which are actions "contrary to the international obligations of [an] injured state vis-à-vis the responsible state if they were not taken by the former in response to an internationally wrongful act . . . to procure cessation and reparation."[91] These countermeasures would not constitute an internationally wrongful act as long as they comply with the requirements for countermeasures under the international law of state responsibility.[92]

A state can also be found responsible for a cyber act through the "non-intervention principle," which refers to perpetrating states compelling other states' affairs.[93] "The International Court of Justice has confirmed that the non-intervention principle is violated, for example, if a state provides financial support, training, a supply of weapons, intelligence, and logistic support to a terrorist or insurgent group operating in another state."[94] Thus, under the non-intervention principle, cyber acts that are committed by non-state actors can be attributable to a state if the state is found to have supplied malware, trained the group on how to administer the malware, and provided support in committing the act. A state may not wittingly allow using its territory to violate other states' rights, whether the act is a traditional kinetic act or a cyber act originating in the perpetrating state's territory.[95] For example, a state would be responsible for shutting down a cyber act committed by non-state actors if the act violated another state's rights. However, whether the state was responsible for the non-state actor's act, to begin with, is a question of attribution.[96]

Generally, the actions of a state that can be attributable to the state depend on whether the entities of the state that are dependent on the state to function are committing the acts.[97] Conversely, actions of private citizens are not attributable to states under international law.[98] The process of attribution for non-state actors depends upon the ability to prove that a relationship exists between the non-state actor committing an internationally unlawful act and the potential perpetrating state.[99] To further complicate the pursuit of attribution, some non-state actors employ malicious cyber acts that do not meet the threshold of an "armed attack" under *LOAC*. These non-state actors also do not fall under the guidance presented in the *Tallinn Manual* in support of their nation-state or their political objectives.[100] With various factors associated with the actor, as

well as the low cost of committing cyber acts, the accessibility of the Internet, and the anonymity inherent in cyberspace, establishing a connection between a state and a non-state actor can be formidable.[101]

LOAC distinguishes between international armed conflict between states and non-international conflict between a state and non-state actors, such as an organized group.[102] Attribution in these cases is critical because of the ability of victim states to respond with the use of force against the state or non-state actors. Additionally, attribution is critical because, if the support of non-state actors by a perpetrating state can be established and meet the elements of proof that make the act attributable to the perpetrating state, then the cyber act can rise to the level of international conflict under *LOAC*.[103] Further, evidence that other states supported non-state actors in another territory in the pursuit of a cyber act that meets the threshold of an armed attack can "internationalize" a conflict that was considered a non-international armed conflict between a victim state and non-state actors.[104] Support of other states is legally significant because the rules under international law then apply to an armed conflict between a victim state and non-state actors.[105]

The difference between establishing state responsibility and a non-international armed conflict becoming "internationalized" is that the "sponsoring state exercises 'overall control' over an organized armed group."[106] Therefore, though an organized armed group could still be considered a non-state actor, a state supporting the organized armed group could attain complete control of the group's objectives, which would make the organized armed group an extension of that state's military objectives. The International Criminal Court found that merely participating in an operation through financial support or equipping the organized armed group was insufficient to categorize the non-international armed conflict into an international armed conflict between states.[107] Rather, the state had to play a role in the organizing, planning, and coordinating of the military objectives to internationalize the original non-international armed conflict between a victim state and an organized armed group of non-state actors.[108] "By this standard, a state which identifies cyber targets for an organized armed group, provides it essential intelligence necessary to launch destructive attacks, or participates in the planning of the group's military cyber operations becomes a party to an international armed conflict with the target state."[109]

It is important to note the distinction between the non-international armed conflict between a state and an organized armed group of non-state actors with an unorganized individual or group of individual non-state actors. In the instance of a cyber act between a victim state and an unorganized group of individual non-state actors, international law requires the perpetrating state

to have a much higher level of control before the act would rise to the level of an international armed conflict between two states.[110] The state would have to direct the non-state actor(s) in perpetrating a cyber act that would reach the threshold of an armed attack under international law against another state's cyber infrastructure to classify the act as an international armed conflict.[111] There have been insufficient cases in which cyber acts that did not meet the threshold of an armed attack were considered to be at the level of an international armed conflict between two states.[112]

Though the complexity of cyberspace can afford states with the ability to use covert means to pursue national security objectives through non-state actors, placing a state with culpability must occur for international law to apply.[113] Though debatable, the reason may be that international law does not provide specific guidance for cyber acts reaching the degree of an armed attack under international law to non-state actors without the involvement of a perpetrating state in the act. As described in detail in the above sections, state responsibility must be justified, and there is guidance as to what constitutes a state's responsibility for an armed attack. However, when a group or an individual not associated with a state commits an act, the victim state cannot rely on the provisions in international law to respond with use of force or self-defense unless the act is attributed to a state.

As a result of the deficiency in international law regarding the issue of non-state actors perpetrating cyber acts against victim states, there is a high probability that perpetrating states will continue to use non-state actors in their attempts to breach the cyber infrastructures of victim states to avoid the consequences associated with international law. Furthermore, states will continue to use non-state actors to "achieve national security and foreign policy objectives" because of the anonymity of cyberspace and ability of states to deny involvement with the cyber activities of non-state actors.[114] As presented in this section, generally, the high level of evidence needed to attribute responsibility to a state or internationalize a non-international armed conflict provides states with the ability to perpetrate without a substantial risk of retaliation.[115]

Analysis

Limitations of Attribution

> *This world—cyberspace—is a world that we depend on every single day . . . [it] has made us more interconnected than at any time in human history.*
>
> --President Barack Obama, May 29, 2009

Nature of Cyberspace. Cyberspace creates an environment that provides global benefits yet simultaneously exploits vulnerabilities anonymously through a simple keystroke.[116] The environment of cyberspace proposes vulnerabilities to a state's national security because of the connections that exist in all facets of the infrastructure. For example, in modern society, the dependence of Internet connectivity is illustrated through the interconnectivity of financial institutions, transportation, power, and other important infrastructures.[117] Since cyberspace is interconnected, there will always be a risk of affecting other states and its citizens because of any action or response to cyber acts.[118]

Deficiency of Law. As explored in detail above, the *LOAC* and other policies, such as the DoD *Law of War Manual* operate in cyberspace under the same principles as traditional, kinetic warfare. The argument is that these same concepts can apply to any domain; however, the new form of warfare in cyberspace does not necessarily fit the traditional kinetic principles of *LOAC*.[119] For example, a cyber act that shuts down a power grid without causing any physical damage to the structure would not necessarily meet the threshold of a cyberattack; however, a bomb that accomplished the same thing would meet that threshold and provide that state with the ability to defend its self under *LOAC*.[120] An armed attack typically requires a higher threshold to legitimize the use of force in self-defense under *LOAC*.[121]

The issue is how to apply this higher threshold in cyber operations when there is ambiguity in the definitions of these thresholds.[122] Furthermore, the current international law provisions do not address the non-physical effects that cyber acts can have and do not provide sufficient laws for the effect that cyber acts can have over time.[123] These effects, not unlike traditional kinetic effects, can have significant consequences to the sovereignty of a state; however, under *LOAC*, they fail to meet the threshold of use of force or armed attack. "The physical damage or harm requirement is only appropriate in a kinetic context, where it is easier to discern when there are kinetic weapons involved."[124] With the problem of attribution in cyberspace, "physical harm or

damage presents a more attenuated, proximate cause rather than a direct cause."[125] Then in the context of *LOAC*, states may not suffer traditional kinetic acts through the principle of distinction but are subject to cyber acts that affect civilians without any protection under international law.[126]

The *Tallinn Manual* was produced to address the deficiency of law as it related specifically to cyber operations; however, the rules outlined in the *Tallinn Manual* are not enforceable in the same manner as *LOAC* and are not accepted by every state under the United Nations.[127] Additionally, the *Tallinn Manual* did not have representatives contribute from many of the countries within the United Nations, such as Russia, China, and other Eastern states.[128] The most severe limitation to overcome with the *Tallinn Manual* is that it does not provide the authority needed to enforce *LOAC* principles redefined under the *Tallinn Manual* in terms of cyber operations.[129]

Additionally, the *Tallinn Manual* does not definitively categorize the definition of an armed attack. The *Tallinn Manual* provides additional guidance by explaining the threshold for an armed attack in more detail. For example, the *Tallinn Manual* states that in order for a cyber act to reach the level of an armed attack and provide victim states with the ability to use force against another perpetrating state in self-defense, the cyber act has to reach a threshold of scale and effect that is parallel to a kinetic armed attack.[130] However, the *Tallinn Manual* explicitly states that "the issue of whether acts of non-state actors can constitute an armed attack absent direction by a state is controversial" and that "traditionally, [United Nations Charter] Article 51 and the customary international law of self-defense were characterized as applicable solely to armed attacks undertaken by one state against another."[131] Therefore, all other cyber acts committed by non-state actors fall under traditional law enforcement and do not constitute an armed attack without attributing the cyber activity to a particular state.[132] A victim state would not be able to use force against another perpetrating state under international law unless the cyber act met the threshold of scales and effects and was attributed to a state. Further, the *Tallinn Manual* "acknowledged the significant uncertainty that exists within the international law community regarding such matters as the degree of requisite organization a group must have (if any) to be capable of mounting an armed attack as a matter of law."[133] There was a distinct divide in the group of experts behind the *Tallinn Manual* as to whether or not a group of non-state actors could be responsible for an armed attack and whether an individual could be responsible for an armed attack even if the group or individual met the threshold of scale and effect, as required, by a perpetrating state.[134]

States have developed doctrine for cyber operations as a way to guide their armed services despite the lack of clarity in international law. Guidance, such

as the *DOD Law of War Manual* details definitions of cyber acts in an effort to formulate an appropriate response. However, internal policies and doctrine are not necessarily helpful in the international community for establishing thresholds for acts that justify the use of force or an armed attack under the United Nations articles 2(4) and 51, respectively.[135] The state must then convince the international community that an act has reached the threshold of a cyberattack or justify a use of force response if the state wants to comply with United Nations charters because of the deficiency in international law regarding cyber operations.

While an assessment of scale and effects is essential in determining appropriate response, equally important is understanding the applicable view of determining whether an armed attack has occurred.[136] Unfortunately, even the experts on the council charged with writing the still recent scholarship of the *Tallinn Manual* could not fully agree on a standard for the determination of an armed attack in cyberspace. They also could not agree on what rights a victim state may have in using force in self-defense against a cyberattack that could not be attributed to a perpetrating state. There is not a definitive law in place regarding the threshold of an armed attack. International scholars in the production of the *Tallinn Manual* have not been able to define the criteria of an armed attack, and the international community has not been able to classify any cyber acts as meeting that threshold. "No international cyber incidents have, as of 2012, been unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack."[137] The assessment of scale and effects is essential, but also equally important is the agreement of the international community in the determination of an armed attack.[138] Further, even the *Tallinn Manual* could not fully agree on the determination of an armed attack in cyberspace or what rights a victim state may have in using force in self-defense against a cyberattack that could not be attributed to a perpetrating state.

Attributing responsibility to non-state actors adds to the complexity of the process of attribution and holding certain entities responsible for hostile cyber acts. The lack of distinction in legal terms, as described above coupled with the lack of definitive evidence to attribute cyber acts to a state creates a level of difficulty that warrants legal requirements. As described in detail above, international law provides governing rules for cyberattacks that meet the threshold of an armed attack and are facilitated by a state. There is not a rule of law or legal guidance on a victim state's rights when a group or an individual not affiliated with another state commits a hostile cyber act unless that group or individual can be linked to a perpetrating state. Despite the ability of non-state actors to perpetrate hostile cyber acts and their potential to cause political discord, as

well as serious legal and political consequences, there are not any provisions within international law to regulate these actions.[139]

Moreover, concepts key to proving a relationship between a state and non-state actors have not been defined in the law of state responsibility. For example, one of the critical components of attributing a cyber act to a state that was committed by a non-state actor is the concept of "acting under the direction or control of a state."[140] An assessment must be conducted to ascertain that direction was provided by the state to a non-state actor, but this concept is not adequately defined under international law.[141] This deficiency creates a problem for victim states attempting to hold a state responsible for the cyber acts committed by non-state actors. The degree of control becomes an important question in this assessment, and the International Court of Justice has provided that the state "must exercise effective control over the non-state actor" to be attributable to a state.[142] "Effective control" has not been defined; though, the term can imply a greater threshold than the general term of control.[143] However, pertaining to instances where this term has come into question, the ability to satisfy this level of control is pursuant to the victim state's ability to prove that the non-state actor(s) were conducting cyber acts on behalf of the perpetrating state.[144]

As presented, key challenges face the international community in the legal representation of cyber acts under international law. One of the main challenges in this area is that there has been difficulty in reaching a consensus across the international community on how to apply traditional laws of armed conflict to cyber acts.[145] Application has led to a lack of expressed guidance in handling hostile cyber acts perpetrated by both state and non-state actors and left important questions as to how to proceed with a proportionate, distinct response. Since *LOAC* does not provide a sufficient definition of an "armed attack" as it relates to acts committed in cyberspace, victim states are forced to rely on their assessment of the act to articulate any response they may consider. The thresholds that exist for the attribution of states and non-state actors are very hard to reach. The more non-state actors exploit cyber vulnerabilities of victim states, the more perpetrating states may choose to support non-state actors covertly, resulting in victim states developing liberal cases for meeting those thresholds.[146] The burden of proof is on the victim state in these cases, and the victim states need evidence on which to base their assessment.[147]

State Sovereignty. A deficiency exists in international law regarding the definitive understanding of whether cyber acts constitute the use of force or an armed attack. However, "there is no question that non-destructive or injurious malicious cyber operations can violate various established international law norms."[148] One example of international law norms that can be affected by

malicious cyber acts is the principle of sovereignty, which "empowers a state to exercise control over cyber infrastructure and activities within its territory."[149] The *Tallinn Manual* agreed that a cyber act causing destruction to a victim state's cyber infrastructure violated the victim state's principle of sovereignty; however, the *Tallinn Manual* did not agree whether a cyber act, such as delivering malware used to disrupt or destroy data in a victim state's cyber infrastructure, should be considered a violation of the victim state's sovereignty.[150]

As explored above, there are particular thresholds required for cyber acts to be attributable to states for both state actions and actions committed by non-state actors. The thresholds of effective control and overall control set a precedent under international law that requires victim states to assess various factors to attribute an act effectively to a perpetrating state. Though cyber acts can propose a significant threat to a victim state's sovereignty, the high threshold for attribution of the perpetrating state's responsibility, as well as the high threshold for the act to reach the level of an armed attack or warrant the use of force under international law incentivizes states to use cyberspace to further their political objectives through the use of anonymous acts and non-state actors. This situation is one of the reasons victim states should include additional factors in their assessment of cyber acts for attribution.

Limited Technology. Another consideration under attribution is the limitations associated with technology and its use to provide information related to the responsibility of cyber acts. Technical attribution is limited by the structure of the Internet. Information traveling through the Internet is typically organized in "packets."[151] These packets are "discrete units of data outfitted with delivery instructions such as destination addresses," including source Internet protocol (IP) addresses.[152] Routers convey these packets to a particular location; however, routers do not confirm that a source address or IP is "genuine."[153] Though the IPs are included in the router's packet of information, these addresses are not always helpful in discerning or verifying the source of the packet of information.[154] Because of these structural features of the Internet, those perpetrating cyber acts against other cyber infrastructures can conceal the originating source of a packet of information.[155]

The use of technological and forensic tools may allow cyber professionals to implicate perpetrators in cyber incidents; however, there may be circumstances in which technical attribution is insufficient given the ease by which perpetrators may mask their identity, evading responsibility for the act. Circumstances may be such that even though technological means determine a particular actor involved, there may be further evidence to consider that may lead to responsibility attributed to a state rather than an individual actor or group. To further complicate this issue, a state may not want to expose the

actor if that effort would undermine the state's efforts politically or expose any use of tradecraft. The social and political aspects can be crucial to a state's decision-making in terms of attribution and response.

Since cyberspace is vast, interconnected, and includes various systems and equipment to process information, hostile or malicious cyber acts can be conducted through many different means. For example, there are Internet-based acts and non-Internet-based acts that require different technical means of attribution.[156] Trying to determine responsibility in Internet-based acts may require three levels of attribution.[157] The levels consist of finding the equipment used in the act, figuring out the owner of the equipment used in the act, and locating the individual or group responsible for the act.[158] Attributing an act cannot rely only on the technical means of finding the equipment used in an act but must also assess who is responsible for the act. The technical aspects of attribution are important to answer first level questions and possibly second level questions in identifying perpetrators, but the third level of attribution may not be solved solely by technological means.

Additionally, there are different types of acts that can cause different types of attribution problems, as illustrated in Figure 1. Figure 1 includes these types of threats: cyber warfare, cyber espionage, brute force attacks, cybercrime, and cyber nuisance.[159] A cyber act can involve several stages that may include gaining control over another computer, network, or system, attacking one computer with another, spoofing IP addresses to disguise the originating machine as another, or harnessing multiple different computers as in the case of a distributed denial of service (DDoS) attack.[160] The type of cyber act should be determined, technical tools should be applied to start the process of attribution, and then an analysis of the type of threat should be implemented. Insight into the type of threat can provide information on other techniques that are needed to conclude responsibility for an act.

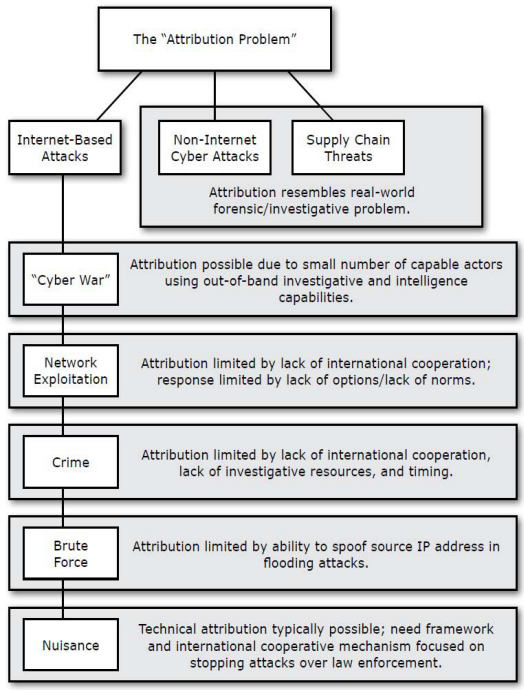

Figure 1: Problem of Attribution[161]

In an interview with Maj Zachary Smith— deputy chief of staff operations, headquarters United States Air Force (A3), Cyber Effects Division— he indicated there were five different main types of threats associated with cyberspace.[162] The five types included: politically-minded hacking, crime, espionage, terrorism, and warfare.[163] Accomplishing politically-minded hacking by non-state actors committing cyber acts is not necessarily reaching the threshold of a crime, but it will advance a political agenda.[164] A crime committed through cyber acts is usually an attempt to exploit information for financial gain.[165] Those actors committing espionage are generally connected to national systems online to gain access to information for adversaries of victim states.[166] Terrorism represents individuals and groups of individuals seeking to commit acts of terror through cyberspace; though terrorism can occur in cyberspace, it does not seem as prevalent as once thought and does not necessarily pose the most significant concern in cyberspace.[167] Finally, cyber warfare is a threat that has very few examples because of the ambiguity in international law.[168] Most cyber incidents can fit into one

of these threat categories, but attribution is the most significant in the case of warfare because of the implications under international law and a victim state's ability to appropriately respond.[169]

Determination of the act is vital because assessing the act establishes the need for attribution. In most cases of cyber incidents, the incidents are not significant enough to reach the level of warfare, and less significant incidents can be categorized as a lower threat. These threat categories allow for more effective threat management against future cyber acts.[170]

"Attribution is necessary in these cases as a response to a cyberattack is often contingent on the nature of the attack and attacker."[171] As discussed above, once an act has occurred, the nature of the act should be considered as a step in the attribution process. For example, a state should assess what kind of cyber operation has occurred, what the potential effects of the act were, what definition does the act meet, and what was the motive behind the act. Each threat can create additional problems in attributing an act to an actor, but assessing the threat can provide leads to identifying the perpetrator. In the case of attribution in cyberspace, the analysis of signatures used through technical and forensic means, as well as behavioral factors in actors, such as an actor's preference for Internet platforms or particular types of spoofing can aid the limiting factors of the technological process for attributing cyber acts.[172]

Introduction into Multi-Dimensional Approach to Attribution

As discussed in previous sections, there are additional factors involved in the attribution process beyond technological or forensic processes. There are different types of cyber acts and actors that are part of the criteria for analyzing the severity of response. Therefore, the process of attribution must require an analysis of the different possibilities of acts and actors that will assist in the decision of what response is appropriate for the initial cyber act. This assessment is imperative in the collection of evidence to attribute the cyber activity to a particular entity or individual. Furthermore, the determination of the source of an act is critical because of the implications the act and actor can have under international law. Though it is necessary to locate the origin of the act, it is also equally important to determine if a non-state actor is connected to and potentially working for a nation-state. As the *Tallinn Manual* states, it is "necessary to consider the issue of the 'originator' in determining whether an act qualifies as an armed attack" and "indisputable that the actions of non-state actors may sometimes be attributed to a State for the purposes of finding an armed attack."[173]

Though international law does not explicitly address cyber acts, the *Tallinn Manual* states there are factors that victim states can depend on in the determination of an armed attack. It involves finding more information than just the location of the source of the act.[174] Among these factors noted, the *Tallinn Manual* states considering property ownership, status of individuals targeted, and the motivation for the specific target should determine whether the act meets the threshold of an armed attack.[175] This determination indicates that there is a need to look beyond the physical implications of an act and that there is value in assessing other factors in attributing a cyber act.

Moreover, these additional factors and considerations can assist victim states in determining whether or not a cyber act is committed by a non-state actor under the control of a perpetrating state. This analysis is crucial in the establishment of an armed attack or an international armed conflict executed through an organized armed group of non-state actors. Without the inclusion of these factors and considerations, a victim state is limited in its ability to respond to a violation of its sovereignty. Since the thresholds under international law are high, not definitively set forth, and technology is limited in its assessment of the originator of an act, non-technical collection of human factors should be considered relevant circumstantial evidence in proving a victim state's case in an international forum, for attributing the cyber act or acts to a perpetrating state.

Factors. Though an understanding of international law and the principles of the law of war are necessary for the context of cyber operations, the law is only part of the attribution equation.[176] In law enforcement, technology and forensics aid law enforcement officials in their pursuit of attribution. However, other human factors that provide critical information in developing the identity of a perpetrator. Similar to law enforcement, human factors are vital in determining attribution in cyber operations against victim states. For instance, deciphering motives behind an incident could provide victim states with valuable information on the responsible party. If attribution were to rely solely on technological means, victim states may uncover an actor, but miss a more significant player involved, such as a state potentially sponsoring the malicious cyber acts to further its political agenda.

Since attribution inherently comes with a degree of uncertainty, the human factors also provide circumstantial evidence to support the attribution to a particular actor or state. The process of attributing a cyber act to a state or non-state actor is a "nuanced and multi-layered process."[177] Therefore, attribution cannot be considered merely a technical problem.[178] It is a social problem in a technically fluid environment meaning that technology alone is not sufficient to attribute a cyber act to a state or non-state actor to the level

required under international law.[179] Accordingly, a multi-dimensional approach that incorporates multiple factors typically used in law enforcement to gather evidence of the nature of the offender is needed to effectively attribute hostile, malicious cyber acts to the appropriate and responsible party.

Additional Considerations. Though human factors are an essential part of the attribution process, other variables are also important in considering a multi-dimensional approach. Other considerations in addition to the type of cyber activity and actors involved are the risk associated with the act and the speed in which attribution can be accomplished.[180] According to Dr. Richard Harknett, head of the political science department at the University of Cincinnati, the lack of certainty in of attributing responsibility to a particular actor exacerbates the need to act.[181] The uncertainty inherent in the attribution process affects decision-making speed. It is essential to consider the degree of certainty in attributing responsibility as a variable in the assessment because this is not addressed in absolute terms under international law and remains a question of what would be considered acceptable to legitimize a response to a cyber act.

Further complicating this issue is the factor of timing.[182] What amount of timing would be necessary to elevate a state's confidence in its attribution assessment from low to high?[183] What consequences would timing have?[184] In terms of shaping an adversary's behavior, the timing of response could have negative consequences.[185]

The additional considerations discussed in this section are only a small amount of potential variables that should be considered in the attribution process. Similar to law enforcement, the analysis of variables leads to more potential information and evidence that can aid in the determination of responsibility for an act. The primary purpose of presenting additional considerations is to provoke thought as to what factors are necessary for victim states to determine what is sufficient to convince in an international court. As in traditional cases of hostile acts, a myriad of evidence is needed to persuade others that a particular party is responsible. The lack of clarity under international law for cyber acts below the threshold of warfare leave victim states with acquiring their elements of proof to protect their sovereignty.

Evidentiary Considerations in Attribution

In attribution, victim states must assess the act, the actor, and any other potential factors that provide information to support the victim state's theory of responsibility for the cyber act. The lack of defined terms and ambiguous thresholds present in international law creates a complex task for victim states

in the pursuit of responding to cyber acts. Attribution is vital to a victim state because responsibility of an act must be determined before a response can be implemented. Further, as described above, international law requires the act to meet a particular threshold in order for a victim state to respond in proportionality. The ability of a victim state to respond is related to the severity of the act.[186] "In principle, the graver the underlying breach, the greater the confidence must be in the evidence relied upon."[187] The reason behind this statement is that with the rise in severity of the act comes a higher risk that the determination of responsibility could produce a proportionate response from a victim state. If incorrectly attributed, it could be devastating to another state.[188] This error is a particularly crucial evidentiary consideration when determining the attribution of a cyber act committed by non-state actors and the attempt to attribute that act to a state.

However, international law does not outline the evidentiary considerations necessary to assess attribution. "Investigations of cyberattacks among states are complicated by the absence of a uniform body of rules on the production of evidence in international law."[189] One of the complications specific to cyberspace is the levels of evidence that are necessary to attribute a cyber operation to a particular state.[190] There may be three levels of evidence. The first level is locating the physical equipment used in the cyber operation.[191] The second level is the identification of the individual(s) behind the cyber operation.[192] The third level is connecting individual(s) to a state, and proving that the individual(s) were acting on behalf of the state is needed to attribute the cyber operation to a state.[193] With technological advances and forensic tools, it seems plausible to determine with accuracy the first level of evidence necessary to attribute a cyber operation to an adversary. However, technology can only assist with the other two levels of evidence. This is the nature of cyberspace. Cyberspace allows adversaries to assume aliases, hide behind various technology, and use other computers to carry out their goals.[194] The International Court of Justice has alluded to the need for "clear evidence" in cases of determining responsibility of cyber acts committed by non-state actors; however, the International Court of Justice did not explain any further as to the meaning or threshold of "clear evidence."[195] Moreover, the standard of proof does not have to meet the criminal standard of "beyond a reasonable doubt" nor does it require absolute certainty.[196] Therefore, victim states must rely on more than just technology to attribute cyber operations to a particular actor.

It is well established that in its very general sense, "attribution is a multidimensional issue that draws on all sources of information available, including forensics, human intelligence, signals intelligence, history, geopolitics, among other" things.[197] Such human factors assist in the attribution of individuals and

groups to a particular state. Circumstantial evidence such as background and associations provide victim states with information that can link an individual or groups to a particular state. These types of factors provide a picture of the party responsible and the likelihood the party is associated with others. In the law enforcement field, an investigator's study of a perpetrator's past affiliations and associations can provide significant leads that can help identify the responsible party behind a particular criminal act. Similarly, attribution can also include the determination if an act was meant to be malicious or hostile in the first place.[198] Additional factors provide an opportunity for states to generate an accurate threat picture that can guide them in the collection of evidence in their case for attribution.

Conclusion

Attribution in the cyber domain can be especially complicated for these reasons: the inherent nature of cyberspace, the deficiency in international law as it relates specifically to cyberspace, the violation of a state's sovereignty and the ability to prove a state's responsibility, and the limitations of technology in attribution. The actor could commit a hostile cyber act in anonymity because of the way the domain is built. A determination of the actor and a thorough assessment of the activities are critical to the victim state's ability to respond to a violation of its sovereignty. For victim states to be able to respond to any violations of sovereignty, the ability to ascertain attribution of malicious cyber operations is essential.

Though many researchers have examined the technical aspect of attribution, the process of attribution is multi-dimensional and requires an investigation into multiple, different factors to determine responsibility. There has been an increase in the number of skilled adversaries, and these adversaries can exploit the uncertainty that is inherent in the judgment of attribution.[199] Without the ability to attribute the act to a particular person or state, "the threat of effective [response] in the cyber domain is an empty one."[200] Specifically, victim states are required to attribute the act before any response can commence because that response must be justified; therefore, there must be an established link between the act, the actor, and the state in which it originated.[201]

Attribution of cyber acts is the responsibility of victim states, and as evidenced in detail above, victim states are required to prove that cyber acts meet certain thresholds. Attributing acts to a perpetrating state must occur in order for international law to apply. Generally, the law provides states with the elements of proof that they must meet to attribute responsibility for a crime; however, as of the writing of international law today, there are not any

definitive elements of proof for victim states to use in their efforts to prove accountability for cyber acts that do not meet the threshold of use of force or armed attack, or prove the accountability of a cyber act to a perpetrating state. Therefore, more research in the definition of specific terms under international law—such as use of force and armed attack—is critical if the attribution problem is to be solved. Furthermore, reaching an international collaboration of understanding in the operation of cyberspace is for not only states but also for explicitly addressing the issue of non-state actors perpetrating cyber acts against victim states.

A consensus of the international community on the definition of terms and legal processes afforded to victim states decreases the amount of ambiguity associated with the process of attribution. As previously explored, there are already issues with attribution as a result of the inherent nature of cyberspace. A more definitive stance written into international law would alleviate the burden of attempting to define the act in addition to finding the actor and then proving involvement with a perpetrating state. Additional research and a push for international consensus may be worth the effort to establish an effective international legal position.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. United States, Department of Defense Office of General Counsel, *Department of Defense Law of War Manual,* (Washington, DC: Department of Defense, December 2016), 986, https://apps.dtic.mil/.
2. US, DoD, Office of General Counsel, *Law of War Manual, 986.*
3. Michael N. Schmitt, "The Law of Cyber Targeting," *Naval War College Review* 68, no. 2 (Spring 2015): 18, https://digital-commons.usnwc.edu/.
4. US, DoD, Office of General Counsel, *Department of Defense Law of War Manual,* 986.
5. "Attribution." Merriam-Webster, https://www.merriam-webster.com/.
6. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (2015): 4, 37. doi:10.1080/01402390.2014.977382.
7. Rid and Buchanan, "Attributing Cyber Attacks," 4, 37.
8. Rid and Buchanan, "Attributing Cyber Attacks," 6.
9. Rid and Buchanan, "Attributing Cyber Attacks," 6.
10. Rid and Buchanan, "Attributing Cyber Attacks," 6.
11. United States. Judge Advocate General's Legal Center and School, US Army, *Law of Armed Conflict Deskbook (*Charlottesville: VA, International and Operational Law Department, 2015), 23, http://www.loc.gov/.

12. US JAG Legal Center and School, *LOAC Deskbook*, 23.

13. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

14. Rid and Buchanan, "Attributing Cyber Attacks," 5-6.

15. US, DoD, Office of General Counsel, *Law of War Manual,* 985.

16. US, DoD, Office of General Counsel, *Law of War Manual,* 986.

17. US, DoD, Office of General Counsel, *Law of War Manual,* 986.

18. US, DoD, Office of General Counsel, *Law of War Manual,* 986.

19. US, DoD, Office of General Counsel, *Law of War Manual,* 986.

20. Joint Publication (JP) 3-12, *Cyberspace Operations*, 30 November 2011, II-5, https://www.doctrine.af.mil/.

21. David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*. (Washington D.C.: National Academies Press, 2010), 28, https://www.nap.edu/read/12997/chapter/4.

22. US, DoD, Office of General Counsel, *Law of War Manual,* 988.

23. US, DoD, Office of General Counsel, *Law of War Manual,* 988.

24. US, DoD, Office of General Counsel, *Law of War Manual,* 988.

25. US, DoD, Office of General Counsel, *Law of War Manual,* 990.

26. Rid and Buchanan, "Attributing Cyber Attacks," 5.

27. US, DoD, Office of General Counsel, *Law of War Manual,* 993.

28. US, DoD, Office of General Counsel, *Law of War Manual,* 995.

29. US, DoD, Office of General Counsel, *Law of War Manual,* 996.

30. Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *The Air Force Law Review* 68 (2012): 167-206.

31. US JAG, Legal Center and School, *LOAC Deskbook,* 23.

32. Mudrinich, "Cyber 3.0," 190.

33. Mudrinich, "Cyber 3.0," 190-191.

34. Mudrinich, "Cyber 3.0," 191.

35. Mudrinich, "Cyber 3.0," 191.

36. Mudrinich, "Cyber 3.0," 191.

37. Eric Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework." *Strategic Studies Quarterly* 8 no. 1 (Spring 2014): 114-132, https://www.airuniversity.af.edu/.

38. US, DoD, Office of General Counsel, *Law of War Manual,* 988.

39. US, DoD, Office of General Counsel, *Law of War Manual,* 989.

40. Schmitt, "The Law of Cyber Targeting," 18.

41. Schmitt, "The Law of Cyber Targeting," 19.

42. US, DoD, Office of General Counsel, *Law of War Manual,* 989.

43. Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs* 70, no. 1 (Winter 2016), 79, https://jia.sipa.columbia.edu/.

44. Mudrinich, "Cyber 3.0," 192.

45. Mudrinich, “Cyber 3.0,” 192
46. Mudrinich, “Cyber 3.0,” 193.
47. Mudrinich, “Cyber 3.0,” 193.
48. Schmitt, ed., *Tallinn Manual 2.0*.
49. Schmitt, ed., *Tallinn Manual 2.0*.
50. Schmitt, ed., *Tallinn Manual 2.0*, 43.
51. Schmitt, ed., *Tallinn Manual 2.0*, 43.
52. Schmitt, ed., *Tallinn Manual 2.0*, 43.
53. Schmitt, ed., *Tallinn Manual 2.0*, 43.
54. Schmitt, ed., *Tallinn Manual 2.0*, 43.
55. Schmitt, ed., *Tallinn Manual 2.0*, 43.
56. Schmitt, ed., *Tallinn Manual 2.0*, 43.
57. Schmitt, ed., *Tallinn Manual 2.0*, 43.
58. Schmitt, ed., *Tallinn Manual 2.0*, 46.
59. Schmitt, ed., *Tallinn Manual 2.0*, 46.
60. Schmitt, ed., *Tallinn Manual 2.0*, 46.
61. Schmitt, ed., *Tallinn Manual 2.0*, 47.
62. Schmitt, ed., *Tallinn Manual 2.0*, 47.
63. Schmitt, ed., *Tallinn Manual 2.0*, 48.
64. Schmitt, ed., *Tallinn Manual 2.0*, 48-49.
65. Schmitt, ed., *Tallinn Manual 2.0*, 52.
66. Schmitt, ed., *Tallinn Manual 2.0*, 52.
67. Schmitt, ed., *Tallinn Manual 2.0*, 52.
68. Schmitt, ed., *Tallinn Manual 2.0*, 57.
69. Schmitt, ed., *Tallinn Manual 2.0*, 57.
70. Schmitt, ed., *Tallinn Manual 2.0*, 57.
71. Schmitt, ed., *Tallinn Manual 2.0*, 58.
72. Schmitt, ed., *Tallinn Manual 2.0*, 58.
73. Schmitt, ed., *Tallinn Manual 2.0*, 58.
74. Schmitt, ed., *Tallinn Manual 2.0*, 58.
75. Schmitt, ed., *Tallinn Manual 2.0*, 60.
76. Schmitt, ed., *Tallinn Manual 2.0*, 60.
77. Schmitt, ed., *Tallinn Manual 2.0*, 60.
78. Schmitt, ed., *Tallinn Manual 2.0*, 61.
79. Schmitt, ed., *Tallinn Manual 2.0*, 61.
80. Schmitt, ed., *Tallinn Manual 2.0*, 61.
81. Schmitt, ed., *Tallinn Manual 2.0*, 97.
82. Schmitt, ed., *Tallinn Manual 2.0*, 97.
83. Mudrinich, “Cyber 3.0,” 193.
84. Mudrinich, “Cyber 3.0,” 193.
85. Mudrinich, “Cyber 3.0,” 193.
86. Mudrinich, “Cyber 3.0,” 195.

87. Michael N. Schmitt and Liis Vihul. "Proxy Wars in Cyberspace: The Evolving International Law of Attribution," *Fletcher Security Review* 1, no. 2 (Spring 2014), 57, https://ccdcoe.org/.

88. Schmitt and Vihul, "Proxy Wars in Cyberspace," 57.

89. Schmitt and Vihul, "Proxy Wars in Cyberspace," 57.

90. Schmitt and Vihul, "Proxy Wars in Cyberspace," 57.

91. Schmitt and Vihul, "Proxy Wars in Cyberspace," 57.

92. Schmitt and Vihul, "Proxy Wars in Cyberspace," 57.

93. Schmitt and Vihul, "Proxy Wars in Cyberspace," 60.

94. Schmitt and Vihul, "Proxy Wars in Cyberspace," 60.

95. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62.

96. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62.

97. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62.

98. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62.

99. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62.

100. Schmitt and Vihul, "Proxy Wars in Cyberspace," 55.

101. Schmitt and Vihul, "Proxy Wars in Cyberspace," 56.

102. Schmitt and Vihul, "Proxy Wars in Cyberspace," 70.

103. Schmitt and Vihul, "Proxy Wars in Cyberspace," 70.

104. Schmitt and Vihul, "Proxy Wars in Cyberspace," 71.

105. Schmitt and Vihul, "Proxy Wars in Cyberspace," 71.

106. Schmitt and Vihul, "Proxy Wars in Cyberspace," 71.

107. Schmitt and Vihul, "Proxy Wars in Cyberspace," 71.

108. Schmitt and Vihul, "Proxy Wars in Cyberspace," 71.

109. Schmitt and Vihul, "Proxy Wars in Cyberspace," 71-72.

110. Schmitt and Vihul, "Proxy Wars in Cyberspace," 72.

111. Schmitt and Vihul, "Proxy Wars in Cyberspace," 72.

112. Schmitt and Vihul, "Proxy Wars in Cyberspace," 72.

113. Schmitt and Vihul, "Proxy Wars in Cyberspace," 55.

114. Schmitt and Vihul, "Proxy Wars in Cyberspace," 72.

115. Schmitt and Vihul, "Proxy Wars in Cyberspace," 72.

116. Zachary P. Augustine, "Cyber Neutrality: A Textual Analysis of Traditional Jus in Bello Neutrality Rules Through a Purpose-Based Lens," *The Air Force Law Review* 71 (2014), 71.

117. Hemen Philip Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analyzing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century." *Baltic Journal of Law & Politics* 10, no.1 (2017), https://www.degruyter.com/.

118. Mudrinich, "Cyber 3.0," 195.

119. Priyanka R. Dev, "'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U. N. Response," *Texas International Law Journal* 50, no. 2/3, (Spring/Summer 2015), 382, https://texashistory.unt.edu/.

120. Dev, "'Use of Force' and 'Armed Attack,'" 396.
121. Dev, "'Use of Force' and 'Armed Attack,'" 395.
122. Dev, "'Use of Force' and 'Armed Attack,'" 387.
123. Dev, "'Use of Force' and 'Armed Attack,'" 388.
124. Dev, "'Use of Force' and 'Armed Attack,'" 390.
125. Dev, "'Use of Force' and 'Armed Attack,'" 390.
126. Dev, "'Use of Force' and 'Armed Attack,'" 390.
127. Dev, "'Use of Force' and 'Armed Attack,'" 383–384.
128. Dev, "'Use of Force' and 'Armed Attack,'" 385.
129. Dev, "'Use of Force' and 'Armed Attack,'" 385.
130. Schmitt, ed., *Tallinn Manual 2.0*, 58.
131. Schmitt, ed., *Tallinn Manual 2.0*, 58.
132. Schmitt, ed., *Tallinn Manual 2.0*, 58.
133. Schmitt, ed., *Tallinn Manual 2.0*, 59.
134. Schmitt, ed., *Tallinn Manual 2.0*, 59.
135. Dev, "'Use of Force' and 'Armed Attack,'" 385.
136. Schmitt, ed., *Tallinn Manual 2.0*, 58.
137. Schmitt, ed., *Tallinn Manual 2.0*, 57.
138. Schmitt, ed., *Tallinn Manual 2.0*, 58.
139. Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law," 12.
140. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62
141. Schmitt and Vihul, "Proxy Wars in Cyberspace," 62
142. Schmitt and Vihul, "Proxy Wars in Cyberspace," 64.
143. Schmitt and Vihul, "Proxy Wars in Cyberspace," 64.
144. Schmitt and Vihul, "Proxy Wars in Cyberspace," 64.
145. Augustine, "Cyber Neutrality," 72.
146. Schmitt and Vihul, "Proxy Wars in Cyberspace," 65.
147. Schmitt and Vihul, "Proxy Wars in Cyberspace," 66.
148. Schmitt and Vihul, "Proxy Wars in Cyberspace," 60.
149. Schmitt and Vihul, "Proxy Wars in Cyberspace," 60.
150. Schmitt and Vihul, "Proxy Wars in Cyberspace," 60.
151. Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility," *Melbourne Journal of International Law* 14, no. 2 (2013): 503, https://law.unimelb.edu.au/.
152. Margulies, "Sovereignty and Cyber Attacks," 503.
153. Margulies, "Sovereignty and Cyber Attacks," 503.
154. Margulies, "Sovereignty and Cyber Attacks," 503.
155. I Margulies, "Sovereignty and Cyber Attacks," 503.
156. Mudrinich, "Cyber 3.0," 199.
157. Mudrinich, "Cyber 3.0," 194.
158. Mudrinich, "Cyber 3.0," 200.
159. Mudrinich, "Cyber 3.0," 201.

160. Margulies, "Sovereignty and Cyber Attacks," 503.
161. Mudrinich, "Cyber 3.0," 197.
162. Maj Zachary Smith (Deputy Chief of Staff-Operations Headquarters United States Air Force, Cyber Effects Division), interview with the author, 4 January 2018.
163. Smith, interview.
164. Smith, interview.
165. Smith, interview.
166. Smith, interview.
167. Smith, interview.
168. Smith, interview.
169. Smith, interview.
170. Smith, interview.
171. Mudrinich, "Cyber 3.0," 197.
172. Margulies, "Sovereignty and Cyber Attacks," 504.
173. Schmitt, ed., *Tallinn Manual 2.0*, 58.
174. Schmitt, ed., *Tallinn Manual 2.0*, 60.
175. Schmitt, ed., *Tallinn Manual 2.0*, 60.
176. Mudrinich, "Cyber 3.0," 195.
177. Rid and Buchanan, "Attributing Cyber Attacks," 30.
178. Dr. Richard Harknett (University of Cincinnati), interview by author, 8 January 2018.
179. Harknett, interview.
180. Harknett, interview.
181. Harknett, interview.
182. Harknett, interview.
183. Harknett, interview.
184. Harknett, interview.
185. Harknett, interview.
186. Schmitt and Vihul, "Proxy Wars in Cyberspace," 66.
187. Schmitt and Vihul, "Proxy Wars in Cyberspace," 65.
188. Schmitt and Vihul, "Proxy Wars in Cyberspace," 66.
189. Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations." *Texas International Law Journal* 50, no. 2/3, (Spring/Summer 2015): 240, https://westminsterresearch.westminster.ac.uk/.
190. Roscini, "Evidentiary Issues in International Disputes," 240.
191. Roscini, "Evidentiary Issues in International Disputes," 240.
192. Roscini, "Evidentiary Issues in International Disputes," 240.
193. Roscini, "Evidentiary Issues in International Disputes," 240.
194. Roscini, "Evidentiary Issues in International Disputes," 234.
195. Schmitt and Vihul, "Proxy Wars in Cyberspace," 66.
196. Schmitt and Vihul, "Proxy Wars in Cyberspace," 66.
197. Lin, "Attribution of Malicious Cyber Incidents," 78.
198. Lin, "Attribution of Malicious Cyber Incidents," 78.

199. Lin, "Attribution of Malicious Cyber Incidents," 129.
200. Mudrinich, "Cyber 3.0," 189.
201. Mudrinich, "Cyber 3.0," 189.

Abbreviations

DDoS	Distributed Denial of Service
DoD	Department of Defense
IP	Internet Protocol
LOAC	Law of Armed Conflict

Bibliography

Augustine, Zachary P. "Cyber Neutrality: A Textual Analysis of Traditional Just In Bello Neutrality Rules Through A Purpose-Based Lens." *The Air Force Law Review* 71 (2014): 69–106.

Clark, David D. and Susan Landau. "Untangling Attribution." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, 25–40. Washington D.C.: National Academies Press, 2010. https://www.nap.edu/read/12997/chapter/4.

Dev, Priyanka R. "'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U. N. Response." *Texas International Law Journal* 50, no. 2/3, (Spring/Summer 2015): 381–401. https://texashistory.unt.edu/.

Faga, Hemen Philip. "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analyzing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century." *Baltic Journal of Law & Politics* 10, no.1 (2017): 1–34. https://www.degruyter.com/.

Guitton, Clement. "Attribution." In *Cybersecurity Policies and Strategies for Cyberwarfare Prevention,* Richet, Jean-Loup, ed., *37–52.* Hershey, PA: Information Science Reference, 2015.

Joint Publication (JP) 3–12. *Cyberspace Operations*. 30 November 2011. https://www.doctrine.af.mil/.

Lin, Herbert S. "Attribution of Malicious Cyber Incidents: From Soup to Nuts." *Journal of International Affairs* 70, no. 1, (Winter 2016): 75–129. https://jia.sipa.columbia.edu/.

Margulies, Peter. "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility." *Melbourne Journal of International Law* 14, no. 2 (2013): 496–519. https://law.unimelb.edu.au/.

Mejia, Eric. "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework." *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 114–132. https://www.airuniversity.af.edu/.

Mudrinich, Erik M. "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem." *The Air Force Law Review* 68 (2012): 167–206.

Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37. doi:10.1080/01402390.2014.977382.

Roscini, Marco. "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations." *Texas International Law Journal* 50, no. 2/3, (Spring/Summer 2015): 233–273. https://westminsterresearch.westminster.ac.uk/.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

_____. "The Law of Cyber Targeting." *Naval War College Review* 68, no. 2 (Spring 2015): 11–29. https://digital-commons.usnwc.edu/.

Schmitt, Michael N. and Liis Vihul. "Proxy Wars in Cyberspace: The Evolving International Law of Attribution." *Fletcher Security Review* 1, no. 2, (2014): 53–72. https://ccdcoe.org/.

United States Judge Advocate General's Legal Center and School. L*aw of Armed Conflict Deskbook.* Charlottesville: VA, International and Operational Law Department, 2015. http://www.loc.gov/.

United States. Department of Defense. Office of General Counsel. *Department of Defense Law of War Manual*. (May 2016): 985–1000. https://apps.dtic.mil/dtic/tr/fulltext/u2/1014128.pdf.