Fordham Undergraduate Law Review

Volume 2 | Issue 1 Article 5

11-2020

The Application and Advancement of International Law: France's New Cybersecurity Policy

Jonathan Katz
Fordham University

NOTE

THE APPLICATION AND ADVANCEMENT OF INTERNATIONAL LAW: FRANCE'S NEW CYBERSECURITY POLICY

*Jonathan Katz**

The prolific growth of technological advancements has undoubtedly improved the quality of life for many, both directly and indirectly. However, the integral role technology now plays in our society presents a plethora of opportunities for the technologically-savvy to exploit; the consequences of such, many world leaders are incapable of dealing with. The 2016 United States Council of Economic Advisers estimated that pernicious operations resulted in losses upwards of fifty billion dollars.[194] Indeed, hackers have intervened in governmental affairs, most notably in the fields of national defense, central infrastructure, and information and communication technologies (ICT). In most cases, these crimes cross international borders. The need for a form of global governance was recognized in light of these increasingly pervasive cybersecurity attacks. In 2019, the French Ministère des Armées (Ministry of the Armies) released four major reports tackling the issue of cybersecurity in the international sphere. The last report, "Droit International Appliqué aux Opérations dans le Cyberespace" (In English: International Law Applied to Operations in Cyberspace)[195] stands out as a watershed document on cybersecurity in international law. Despite its apparent ambiguity, it pushes the global understanding of international law as a powerful tool to mediate crises such as cybersecurity threats. The document has established itself as a precedent and can be expected to influence other countries in the upcoming months.[196]

---

* B.A. Candidate for International Political Economy, Fordham College at Rose Hill, Class of 2023. The opportunities provided by the Fordham Undergraduate Law Review and its leadership are both innumerable, and invaluable. Their unwavering selfless support has allowed their members to flourish and set the publication on a path for continued success. On a more personal note, I would like to thank former Co-Managing Editor Naomi Izett for her continued support, guidance, and oversight throughout the drafting and editing processes. Without her, overcoming the complexities of international law would not have been possible. Lastly, infinite thanks are due to my family whose continued support allows me to engage in such rewarding opportunities.

[194] *The Cost of Malicious Cyber Activity to the U.S. Economy*, The Council of Economic Advisers (February 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[195] Ministère des Armées, La Fabrique Défense (2017-2019), https://www.defense.gouv.fr.

[196] Shortly after publication of France's newest policy (December 2019), the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was called to discuss the

I. INTRODUCTION

The comprehensive policy outlined in the *International Law Applied to Operations in Cyberspace* draws primarily on two defining characteristics of international law: sovereignty and customary law. While these principles are

application of international law to cybersecurity operations. Harriet Moynihan, *The Application of International Law to Cyberspace: Sovereignty and Non-Intervention,* Just Security, (December 13, 2019), https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/.

widely accepted by most states, their inherent ambiguity can sometimes be the cause of disputes.

The principle of sovereignty first arose in 1648 at the end of the Thirty Years' War which spawned the need for international regulations due to the creation of numerous inclusions of numerous European provinces and states. The Peace of Westphalia yielded two fundamental characteristics of international law; the right to sovereignty and the right to a national identity.[197] The definition adopted at the time was influenced mostly by positivist thought which asserted that a state's right to govern itself was the supreme law, and no moral authority could exist above it. The idea of sovereign states has faced significant opposition by those who believed in what is known as natural law, which promotes general goodwill between nations based on preexisting philosophical and religious principles.[198] Centuries later, the mass atrocities committed during the Second World War would tip the scale in favor of the natural law interpretation.

This, paired with the formation of the United Nations (UN), created a platform for the development of principles to govern globalization in a increasingly interdependent world.[199] Customary law is the fabric that holds international principles and treaties together. It developed to fill in the "gray areas" caused by the ambiguity of international laws. It represents the commonly accepted international etiquette of politics. While it is by nature more flexible it is recognized as a unique but powerful tool used by international lawyers. Customary law and Sovereignty are often viewed as important ideas which guide international law. This is undoubtedly why France decided to use these widely recognized principles to support their doctrine.

II. THE USAGE OF SOVEREIGNTY IN *DROIT INTERNATIONAL ALLIQUE AUX OPERATIONS DANS LE*

The application of international law towards operations conducted in cyberspace is as novel as the development of cyberspace itself. As society develops, it looks to international law to guide the legal precedents that will shape future international politics. But what provides structure to these doctrines? The first is one of the most debated concepts in international law: sovereignty. Presumably, nations would look to the UN, the principal

[197] David and Keitner Bederman, Chimene, International Law Frameworks (Concepts and Frameworks, Foundation Press (February 24, 2016).
[198] *Id.*
[199] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Introduction and General International Law in Cyberspace*, Cambridge University Press (2017).

international governing body, to define such a term. However, the UN has avoided issuing a concrete definition of sovereignty. Article 2.1 of the UN Charter highlights that "the organization is based on the principle of the sovereign equality of all its Members."[200] Despite ongoing lack of clarification regarding the term, consensus among states finds that sovereignty is viewed as "the principle that each State answers only to its own domestic order and is not answerable to a larger international community, except to the extent it has consented to be."[201] Many UN member states accept these conditions, one of which is being open to external intervention under specific circumstances. The definition purposefully leaves that open to interpretation, as is customary with international law. France, along with other nations before it (See Section V: *A,B,C,D,E)*, have used the ambiguous definition of sovereignty to develop necessary international cyberspace policies that fall within the scope of international law.

III. THE USAGE OF CUSTOMARY IN *DROIT INTERNATIONAL ALLIQUE AUX OPERATIONS DANS LE CYBERSPACE*

The definition of sovereignty accepted by the international community is an example of customary law at work. The ability for customary law to shape the international political landscape while not necessarily being concrete, has only further emphasized its importance to the international community. The International Court of Justice (ICJ) under Article 38 describe the effectiveness of customary law:

> Custom is 'evidence of a general practice accepted as law.' To show a rule of customary international law, one must prove to the satisfaction of the relevant decisionmaker (whether an international tribunal, a domestic court, or a governmental or inter-governmental actor) that the rule (1) has been followed as a 'general practice,' and (2) has been 'accepted as law.'[202]

The guiding principles of international law are the only common principles accepted. These general practices have served to advance international law only to the extent that it need be. While, as a whole, international law has proven to be ambiguous, customary law has served to add clarity. A specific example of this can be seen with operations occurring in cyberspace.

---

[200] Charter of the United Nations: Chapter 1, United Nations (2019), https://www.un.org/en/sections/un-charter/chapter-i/index.html.
[201] A/C.1/73/L.27, United Nations (October 2018), https://undocs.org/A/C.1/73/L.27.
[202] David and Keitner Bederman, Chimene, International Law Frameworks (Concepts and Frameworks, Foundation Press (February 24, 2016).

IV. IS A DOCTRINE CONCERNING INTERNATIONAL CYBERSPACE SECURITY APPLICABLE TO INTERNATIONAL LAW?

International law is vast and complex. However, it can often be guided by the two defining characteristics discussed above: sovereignty and customary law. France's doctrine is not the first time these characteristics have formulated international policy; they have long been ingrained in international law. Multiple mass atrocity crimes committed within the last century have had rippling effects on politics and policies on a global scale, each greater than the last. It is in support of this precedent that France has constructed its doctrine which questions the role international law should play in cybersecurity operations.

As is often the case with internationally applicable legal documents, sovereignty is the linchpin of the ruling. France derives its perception of proper jurisdiction from the Group of Governmental Experts (GGE) and ICT. France assumes responsibility for its cyberspace, similar to how they would for a municipality within its designated international borders. France assumes total control over it and will carry out whatever means it deems necessary to ensure its sovereignty. Any successful cyberattack that permeates, "State digital systems, affects the military or economic power, security or survival capacity of the Nation, or constitutes interference in France's internal or external affairs, will entail defensive cyber warfare operations that may include neutralization of the effect."[203] France's new cyberspace doctrine applies appropriately to the above definition of sovereignty.

In the case of operations occurring in cyberspace operations, like other international relations, 'general practice' is difficult to define. The rapid development of technology has made a customary adoption of principles challenging to abide by. However, four of the five members of the UN Security Council have been able to formulate cybersecurity doctrines that are formulated from many of the same principles. France's doctrine follows a number of these important precedents, the most notable being the customary definition of sovereignty.[204] Furthermore, the doctrine draws on the commonly accepted practices of *jus in bello* (International Humanitarian Law/IHL) when discussing what cyber-attacks may be categorized as an armed conflict, which is also described under customary law to some extent (some portions are defined, but the adaptation for it to fit under cyber-attacks is new). The UN has drawn upon the customary laws followed by many of its member-states. And in the case of cybersecurity, has used the various

[203] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Introduction and General International Law in Cyberspace*, Cambridge University Press (2017).
[204] Ministère des Armées, La Fabrique Défense (2017-2019), https://www.defense.gouv.fr.

doctrines to formulate international policy.[205] Thus, *International Law Applicable to Operations in Cyberspace* and other doctrines concerning cyberspace are not only applicable to international law but are crucial in order to suit the needs of a technologically advanced global society.

V. ADDITIONAL INTERPRETATIONS ON CYBERSPACE, SOVEREIGNTY, AND AMBIGUITY

Before further exploring the question of ambiguity, it is worth analyzing cybersecurity doctrines released by other nations prior to France's. The document, while not the first of its kind, has set the most influential precedent. France's fellow members of the United Nations Foreign Security Council have offered their perspectives.

A. The United Kingdom of Great Britain and Northern Ireland (UK)

In May of 2018, Attorney General Jeremy Wright made a speech to the public titled "Cyber and International Law in the 21st Century". Many of his remarks drew on the United States' *Department of Defense Law of War Manual* which would later be used to help draft *National Cyber Strategy of the United States of America*. Wright made aggressive claims that cyber operations merited physical countermeasures. Additionally, they negate the widespread view that countermeasures need to be announced prior. To protect and prevent violations of sovereignty, the speech outlines decisive, yet ambiguous means for such. As is seen in France's doctrine, certain "gray areas" regarding when a breach of sovereignty merits physical force is prominent throughout.[206]

B. The United States of America (US)

The United States of America (US): In September of 2018, President Donald J. Trump released the *National Cyber Strategy of the United States of America.* The document stood diametrically opposed to the goals regarding cyberspace laid out by the previous presidential administration. Focus has shifted from strictly defensive to offensive. The document promotes the use of preventionist policies in order to maintain security of the nation's populous. Such change is affected by partisan differences however, evolving

[205] Detlev Wolter, *The UN Takes a Big Step Forward on Cybersecurity* https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity.
[206] Jeremy Wright, *Cyber and International Law in the 21st Centur*y, Attorney General's Office (May 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

global perspectives are observable. The document builds off pre-existing cyber doctrine (such as the United Nations Convention Against Trans-National Organized Crime and the G7 24/7 Network Points of Contact).[207] Such advancement of prevention is reminiscent of neo-liberal interpretations on the Responsibility to Protect doctrine and its role of intervention. Similar to the UK, while the doctrine is largely decisive, it leaves a great deal of doctrine up for interpretation.

C. The Russian Federation (RU)

In October of 2018, RU proposed "A/C.1/73/L.27" which was meant to counter the American doctrine adopted a month prior. Instead of promoting effective countermeasures, they maintain the need for "cyber sovereignty" and a nation's need to take care of their own cyberspace. Additionally, instead of encouraging cooperation from the private sector (as is the case with the US doctrine), it is deemed as unimportant.[208] Whether or not one may believe this exclusion due to "unimportance" is debatable, but it seems to discourage the private sector's participation in cyberspace. In response, the United States proposed "A/C.1/73/L.37" as a means of implementing their national doctrine in the international community.[209]

D. The People's Republic of China (CN)

Besides expressing support for its fellow Shanghai Cooperation Organization (SCO) member Russia on "A/C.1/73/L.27", the CN government has remained silent. They have neither confirmed nor denied whether or not international law is applicable in cyberspace.

E. The Republic of France

France does not stray far from the perspective of its allies and often builds upon their doctrine. The focal point of each doctrine is sovereignty (as is often the case with policy concerning international law). Furthermore, general cases in which this sovereignty may be violated are detailed. Yet, a problem arises from this generality. Vague doctrine allows for vastly different interpretations and speculation regarding what is, and is not, protected in regard to sovereignty. However, vague doctrine and concrete doctrine both

[207] *National Cyber Strategy of the United States of America*, The White House (September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[208] A/C.1/73/L.27, United Nations (October 2018), https://undocs.org/A/C.1/73/L.27.
[209] A/C.1/73/L.37, United Nations (October 2018), https://undocs.org/A/C.1/73/L.37.

suffer from shortfalls. If any country were to develop specific rules, failure would surely follow. The scope that international law covers, in combination with the ever-expanding cyberspace, would make developing concrete doctrine ineffective as it would soon become obsolete.

VI. AN INTRODUCTION TO AMBIGUITY

While the seventeenth century gave birth to international law, it would not be until the mid-twentieth century that it would begin to flourish. Due to the rapid development of humanity, international law has always found a need to continually develop. Its horizons are ever-expanding.[210] Political developments often out-pace the legislation of laws. Thus, the scope of international law has always been broad and lacking specificity. As noted previously, sovereignty and customary laws are byproducts of this ambiguity. The definition of sovereignty has never been fully denoted by the UN, or any international governing body that has preceded it. Lack of specificity in situations such as this enhanced the importance of customary law and its role in international politics. General guidelines and principles come to be accepted out of pure necessity in order to seek balance between rapid global changes and slow-moving legislative adaptations. An ambiguous approach to international law has long been contested especially because it is not enforceable. For example, the Responsibility to Protect (R2P) doctrine passed by the UN was designed to eliminate reliance on a system of etiquette and aimed to create concrete rules.[211] Just as ambiguity is not without its detractors, the questionable performance of R2P has fostered its own share of controversy. Due to this, these concurrent questions of enforceability and applicability, the debate between ambiguous versus concrete international doctrine has proliferated.

In the case of France, its doctrine neglects to define "effects" in regard to consequences initiated by foreign cyberspace attacks. While this is not the first international law doctrine to be fraught with ambiguity, it only builds upon already ambiguous principles of cybersecurity (which are defined below). How it "affects" and the resulting "effects" are mostly not definitive throughout this section. Section 1.1 repeatedly refers to specific "effects" as constituting retaliation, even on an international scale. They namely apply to cyber operations that somehow manifest tangible results, such as "large scale

---

[210] H. M. Griffioen*, Some Philosophical Struggles with an Ambiguous Phenomenon*, European Academy of Legal Theory (2001-2002), http://www.dhdi.free.fr/recherches/theoriedroit/memoires/griffioenmemoir.htm.

[211] General Assembly resolution 63/308, *The Responsibility to Protect,* A/RES/63/308, (7 October 2009).

loss of life or considerable economic damage."[212] However, the availability and capabilities of malicious cyber-attacks range far beyond this. Perhaps one of the most common cyberattacks perpetrated today that is not discussed is a Distributed Denial of Service attack (known as a DDoS attack). The United States Department of Homeland Security states "all organizations that rely on network resources are considered potential targets."[213] France, which relies on network resources, would thus be considered a target. However, such attacks are prone to causing delays and inaccessibility when they are carried out. As to matters about those stated strictly by France, there is not necessarily a correlation. The problem with 'general practice' in regard to cybersecurity is that when France chooses to make physical intervention a countermeasure to cyberattacks, it opens a Pandora's Box of potentially detrimental consequences. As technology develops and cyber threats evolve and change, there can be no customary principle accepted by all nations regarding how to respond to perceived threats.

VII. AMBIGUITY: A NECESSARY EVIL

The idea of ambiguity is, in itself flawed, but not nearly as much as establishing concrete doctrine. Ambiguity regarding France's doctrine is reminiscent of the fight to expand the scope of the Responsibility to protect through the adoption of more liberal doctrine. The French doctrine, along with its predecessors, is admittedly, plagued by ambiguity in regard to countermeasures. However, its description of sovereignty violations is strongly supported with evidence beyond the typical "UN Charter" argument. Additionally, it sets up guidelines that provide the ability to physically intervene as a response to cyberspace attacks. While both the US and UK have mentioned these ideas, France is the first nation to specifically focus on such in their document making it a direct goal of the report. Yet, its ambiguity regarding countermeasures raises questions.

Perhaps the case arises in which a DDoS (Distributed Denial of Service) attack is carried out and makes government systems inaccessible for a short period of time, but nothing pertinent to national security. Could the use of what the nation considers a "legitimate" attack be skewed to justify an otherwise unjustified intervention? In this case, where France sees physical intervention as a just retaliation to detrimental cyberattacks, such physical

[212] Michael N. Schmitt, Tallinn *Manual 2.0 on the International Law Applicable to Cyber Operations, Introduction and General International Law in Cyberspace*, Cambridge University Press (2017).
[213] Distributed Denial of Service Defense, U.S. Department of Homeland Security, https://www.dhs.gov/science-and-technology/ddosd.

interventions could occur. Not only does this pose issues concerning France's response, but additionally it does not take into consideration if retaliation is justifiable in international law. The argument could be made that an intervention (posed as a retaliation) could also qualify as a violation of the target state's sovereignty. But there is a definite need for ambiguity and open interpretation. France, the United Kingdom, and the United States have all developed similar doctrines regarding operations in cyberspace. They are based upon similar definitions of sovereignty and take similar steps regarding breaches. However, certain parts are ambiguous and for good reason. The most important part of this multilateral process of international law is that these three nations all follow the same thought-process regarding violations of sovereignty and how to respond, regardless of whether or not the latter is ambiguous. This, in turn creates a customary law of ambiguity and interpretation regarding countermeasures to malevolent cyberspace operations against a given state.

France's move to follow in the footsteps of others has reaffirmed customary law regarding cyber security and physical intervention as a means of retaliation. However, this does not mean it should be left as is. This could possibly lead to rapid escalation of certain crises and presents an extremely delicate balance left up to individual nations. Individual nations are responsible for keeping the doctrine in check. The comprehensive cybersecurity models of these three members of the UN Security Council (backed by a large number of fellow UN members) is pushing the global community towards a more comprehensive cybersecurity model.

VIII. THREE IMPORTANT QUESTIONS

The previous sections have discussed France's doctrine and its application to international law in its current state. The doctrine does draw on pre-existing principles and doctrine and is firmly in accordance with international law. However, does it contribute anything new or meaningful to questions concerning international law? The following three questions developed by Harold Hongju Koh, Legal Advisor for the U.S. Department of State have been repeatedly referred to in discussions on cyberspace and its application to international law. Each question will be examined and then the manner in which *International Law Applicable to Operations in Cyberspace* answers, or fails to answer, will be discussed.

A. How can a use of force regime take into account all of the novel kinds of effects that states can produce through the click of a button?

The French have established that operations conducted in cyberspace apply to international law. Thus, their approach regarding retaliation is rooted in its governing authority: the UN. Two important sections of the UN Charter are stated which instruct how France may interpret and respond with countermeasures.

1. Article 2, Paragraph 4

All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[214]

2. Article 51

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[215]

France has adopted previously accepted principles of international law and applied them to their operations in cyberspace. Through the inclusion of sovereignty and customary law, France proves that its doctrine is built on two pillars of international law. This reflects previously adopted cybersecurity doctrine from both France and its international partners. Their doctrine reinforces the idea cybersecurity doctrine is applicable on an international scale. Furthermore, they reason that since cybersecurity doctrine is applicable under international law, their retaliation procedures are justified as long as they follow pre-existing doctrine regarding such. So, not only is cybersecurity doctrine applicable on an international scale, but France's specific doctrine is applicable cybersecurity doctrine.

In and of itself, France's approach is logical and is in agreement with the previously discussed questions. And, in this manner, it is are not alone. The United States has followed a similar path in their adoption of *jus ad bellum* and its application to cyberwarfare. Both documents aim to apply old

[214] Charter of the United Nations: Chapter 1, United Nations (2019), https://www.un.org/en/sections/un-charter/chapter-i/index.html.
[215] *Id.*

doctrines to new problems. Nevertheless, this presents the adoption of ambiguous principles. Koh states that these ambiguities are nothing new and have existed for many years, especially regarding inter-state diplomacy.[216] A history of ambiguity, combined with the adoption of these previous principles, is observable in the French doctrine as well. The need for ambiguity exists solely for the fact that the world rapidly changes and, with a lack of cohesive thought between states, such a concrete consensus is increasingly difficult to achieve. France takes a definitive stance regarding retaliation in accordance with international law precedents, and it is possible that other countries will follow suit. However, for the time being, they do not appear to have inspired any further advancements in international cybersecurity law.

B. What do we do about "dual-use infrastructure" in cyberspace?

Dual-use infrastructure refers to certain cyber systems that employ both a governmental and civilian use. These are lawful targets under international law, according to Groups of Governmental Experts and those rules that have been accepted under international law.[217] However, the civilian implications of such targeted attacks raise questions regarding International Humanitarian Law. Interpretations on dual-use infrastructure have presented two major questions, one for the offensive and one for the defensive state: What if an offensive state protected its military infrastructure by surrounding it with civilians? What is a defensive state to do if its military objectives are already in civilian areas?

Is there not a possibility of specifically targeted attacks on these areas to maximize human suffering? France focuses a significant portion of their document on these issues. In Section 2.2.2 "Application of the principles governing the conduct of hostilities," France sets forth an important precedent. Defining a military environment in cyberspace is an increasingly difficult task for a state, and its civilian implications could be unprecedented. France elaborates on distinction, specifically between both military and civilian objectives, and the military and civilians themselves. Additionally, they highlight the important distinction between proportionality and precaution especially when attempting to justify military action that may result in civilian casualties.

When defining military targets, "the essential aim of the digital targeting process is to comply with the military objective criterion in terms of

[216] *Id.*

[217] Michael N. Schmitt, Tallinn *Manual 2.0 on the International Law Applicable to Cyber Operations, Introduction and General International Law in Cyberspace*, Cambridge University Press (2017).

distinction, given the nature of the targets (digital systems and infrastructure)".[218] In regards to targeting of dual-use infrastructure, "the non-lethal nature of cyber weapons and the possibility of limiting their effects to a previously identified system contribute to the obligation to choose the means and methods of attack most likely to avoid, or at least reduce to a minimum, any incidental loss of civilian lives, injury to civilians or damage to civilian objects".[219] France inherently uses slight ambiguities throughout such, but overall compiles a doctrine in accordance with *jus in bello* that aims to minimize the overall loss of life in regards to operations occurring against, and by, the state. Not only does France comply, but repeatedly refers to minimizing civilian casualties while simultaneously ensuring their sovereignty.

C. How do we address the problem of attribution in cyberspace?

Attribution in cyberspace is left to the responsibility of individual states. The ability to attribute in cyberspace is subject to the ability of a state to do so. The question does not concern international law directly. International intervention based on attribution is. Again, the topic is characterized by ambiguity through multiple governmental organizations.[220] Individual states are responsible for locating the source of an ambiguous attack in order to respond effectively. Cyberspace exacerbates the ability to respond based on plausible deniability as the laws surrounding it are not clearly defined. France aims to adopt a state-focused policy for attribution in Article 1.3. Such attribution includes characterization of the attacks (both technically and their origin), its implications, and what countermeasures may be taken in accordance with IHL and the policy as a whole. By participating in a definitive process of considering attribution, along with encouraging participation from fellow states in doing so, the doctrine has assisted in reducing the chances of an incorrectly attributed attack.

IX. CONCLUSION

While sovereignty and customary law are the two shining pillars in international law, the third duller pillar, ambiguity, tends to have just as much importance. Despite criticism, the importance of ambiguity should not be understated. Humanity often develops faster than international lawmakers can pen the next important policy. Thus, the nations of the world are self-

[218] Ministère des Armées, La Fabrique Défense (2017-2019), https://www.defense.gouv.fr.
[219] *Id.*
[220] *See* Harold H. Koh, *International Law in Cyberspace*, U.S. Department of State (September 2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

accountable when the international community has not taken a stance on say, cybersecurity. These nations have no guidelines to follow beyond what other nations have said, if anything at all. National policies drafted at these times must remain ambiguous so that they may not only apply to developments in the present, but for the foreseeable future as well. Yet, nations should not continually develop more and more ambiguous policies as such could lead to detrimental consequences. For example, in Section VI. An Introduction to Ambiguity, the idea that an inconsequential threat could lead to an unequal retaliation is proposed. The ability to retaliate on a scale larger than necessary (due to ambiguity) is not impossible. Luckily, large-scale retaliation of a physical nature is regulated by the UN and often subject to international scrutiny. However, this does not mean that the argument could not be made that if France were to retaliate on a large scale, they would not be justified under their recent doctrine.

France has assuredly aligned themselves with the history of International Law and International Humanitarian Law through the adoption of sovereignty, customary law, and ambiguity. Despite adopting a traditional approach on ambiguity, France has eliminated loopholes caused by previously enacted policies regarding dual-use infrastructure. This, and other new outlooks from France, come together to make the doctrine an important precedent to be followed in coming years. The doctrine is largely flexible regarding technology and cybersecurity, but decisive when it comes to protecting the lives of civilians.

* * *