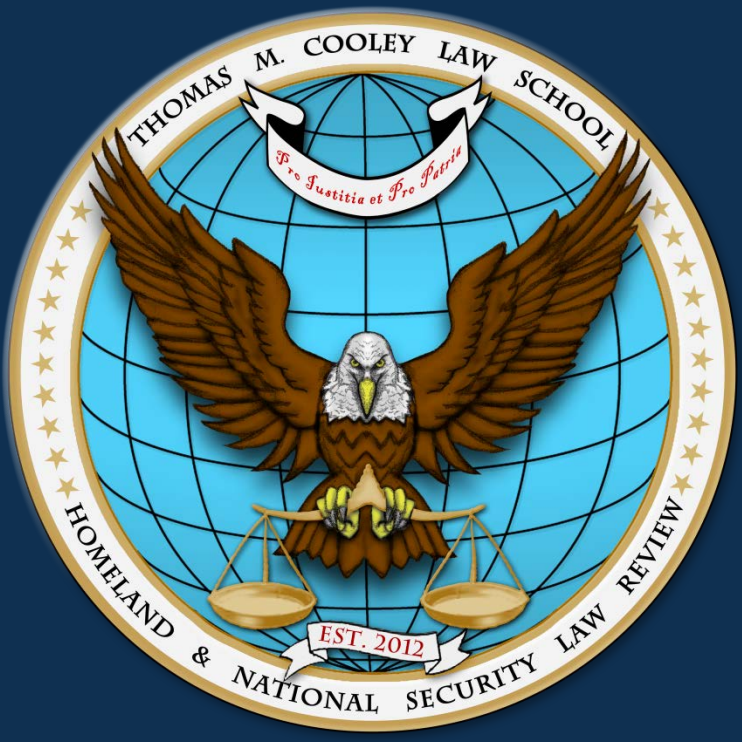
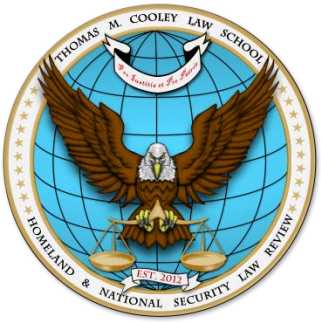
THOMAS M. COOLEY LAW SCHOOL

HOMELAND & NATIONAL SECURITY LAW REVIEW



Articles by
Katherine Vessels
Stefan Ducich
David J. Ryan

FALL 2018 VOLUME 6 ISSUE 1



HOMELAND & NATIONAL SECURITY LAW REVIEW
Thomas M. Cooley Law School
300 S. Capitol Avenue
P.O. Box 13038
Lansing, MI 48901

http://homelandsecuritylawreview.cooley.edu

HOMELAND & NATIONAL SECURITY LAW REVIEW

ARTICLES

FALL 2018 VOLUME 6 ISSUE 1

HOMELAND & NATIONAL SECURITY
LAW REVIEW

FALL 2018 VOLUME 6 ISSUE 1

May 2017-Present
EDITORIAL BOARD

HOMELAND & NATIONAL SECURITY LAW REVIEW

FALL 2018 VOLUME 6 ISSUE 1

Cite as 6 HOMELAND & NAT'L SECURITY L. REV. __ (2018)

The HOMELAND & NATIONAL SECURITY LAW REVIEW (HNSLR) is the first legal periodical by an LL.M. Program at Thomas M. Cooley Law School, in Lansing, Michigan. It is published biannually in digital form. Our mission is to publish timely, practical, and innovative scholarly articles and comments in the field of homeland and national security law. We will also publish a special edition, at least annually, on the legal issues of our Nation's veterans. We strive to foster an intellectual forum for academics and practitioners in the field of homeland and national security law so that others may continue to learn and share in this ever-increasing study of law.

The Editors of HNSLR can be contacted at:

Homeland & National Security Law Review
Thomas M. Cooley Law School
300 South Capitol Avenue
Lansing, Michigan 48901

http://homelandsecuritylawreview.cooley.edu
HNSLawReview@cooley.edu

Submissions: Articles and comments submitted to the HNSLR Editors must be fully researched and of original thought. Footnotes should follow the form prescribed in The Bluebook: A Uniform System of Citation (19th ed. 2010). The HNSLR seeks submissions that will contribute to the field of homeland and national security law.

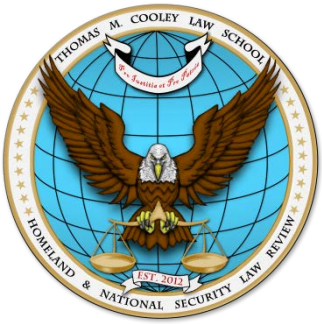
Articles, Comments, and other editorial correspondence should be addressed to the HNSLR Articles Editor by e-mail at HNSLawReview@cooley.edu.

HOMELAND & NATIONAL SECURITY
LAW REVIEW

FALL 2018 VOLUME 6 ISSUE 1

TABLE OF CONTENTS

ARTICLES



PREVENTION PARADOX: WHY THE LOGICAL NATURE OF THE MASS ATROCITY PREVENTION AND RESPONSE OPTIONS (MAPRO) POLICY PLANNING HANDBOOK IMPEDES CHANCES OF PREVENTION

Katherine Vessels

I. INTRODUCTION

Zen Buddhist masters often employ paradoxical riddles, or *koans*, to teach their students the difficulty of describing the nature of a thing through words.[1] These lessons demonstrate to the students that some paradoxes cannot be solved through logical reasoning. In fact, attempting to apply logical reasoning to analyze the nature of a thing can only make it seem more paradoxical.[2] To demonstrate how understanding the nature of a thing cannot be gained by using logical reasoning and language, Zen masters commonly pose the following *koan* to their students, "You can make the sound of two hands clapping. Now what is the sound of one hand?"[3] Through *koans*, the master teaches the student that a holistic approach to thinking about a problem should be applied or the nature of the person answering the question must change.[4]

[1] FRITJOF CAPRA, THE TAO OF PHYSICS: AN EXPLORATION OF THE PARALLELS BETWEEN MODERN PHYSICS AND EASTERN MYSTICISM 43 (5th ed. 2010).
[2] *Id.*
[3] *Id.* at 49.
[4] *See id.* at 43.

Mass atrocities are paradoxes. They seem illogical, absurd, and self-contradictory. After atrocities end, many wonder: What could cause this to happen in our time? How could a functioning government allow this to happen? How could those in power hate a group so much to order their destruction? How could the lower-level perpetrators follow through with such heinous actions? How could the rest of the people stand by and let the perpetrators act with impunity? Why did no one stand up and protect the victims? All of these are *koans* in a new context. One can neither understand the nature of a hand through its sound[5] nor can one understand the nature of mass atrocity through the motivations of its individual actors. Prevention of mass atrocities presents an even greater paradox: If you cannot understand the nature of mass atrocity, how can you shape your efforts to impede or even defeat it?

The Responsibility to Protect doctrine[6] catalyzed this drive for prevention. The doctrine's second and third pillars[7] allow the international community to intervene if a state fails to protect its population from mass atrocities.[8] Prevention, rather than response, emerged as the preferred method of intervention.[9] The United

---

[5] *See* CAPRA, *supra* note 1, at 49.

[6] INT'L COMM'N ON INTERVENTION & STATE SOVEREIGNTY, THE RESPONSIBILITY TO PROTECT, XI (2001) http://responsibilitytoprotect.org/ICISS%20Report.pdf.

[7] "Each individual State has the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity." 2005 World Summit Outcome, Pillar I, G.A. Res. 60/1, para. 138, U.N. Doc. A/RES/60/1 (Sept. 16, 2005); "The international community should, as appropriate, encourage and help States to exercise this [responsibility to protect] responsibility . . . ." *Id.* at paras. 17-69; "The international community, through the United Nations, also has the responsibility to use appropriate diplomatic, humanitarian and other peaceful means, in accordance with Chapters VI and VIII of the Charter, to help protect populations from genocide, war crimes, ethnic cleansing and crimes against humanity." *Id.* at para. 139. While the premises for the pillars were first communicated in the 2005 World Summit Outcome, they were not separated into the three pillars until the Secretary-General's 2009 Report on Implementing the Responsibility to Protect. U.N. Secretary-General, Implementing the Responsibility to Protect: Rep. of the Secretary-General, para. 44, U.N. Doc. A/63/677 (Jan. 12, 2009) [hereinafter Responsibility to Protect].

[8] *See* Responsibility to Protect, *supra* note 7, at 1-2.

[9] U.S. ARMY PEACEKEEPING & STABILITY OPERATIONS INST., MASS ATROCITY PREVENTION AND RESPONSE OPTIONS: POLICY PLANNING HANDBOOK 3 (2012)

States recognized that its planning efforts focused on the response to atrocities and not on prevention.[10] This Paper describes and critiques the Mass Atrocity Prevention and Response Options (MAPRO) Policy Planning Handbook (the Handbook) that resulted from the U.S. efforts to address this planning shortfall.[11] The Handbook provides a foundation for future policy development and recommends a planning process that suggests prevention can be accomplished through action-reaction operations.[12] The paradoxical nature of prevention does not lend itself to linear, logical reasoning, and this Paper demonstrates the flaws in the U.S. logic and how such reasoning will impede prevention efforts.

II. THE U.S. PREVENTION *KOAN* AND THE MAPRO'S ASSESSMENT TOOLS

In 2011, U.S. President Barack Obama issued a Presidential Study Directive on Mass Atrocities.[13] His directive tasked federal agencies with compiling the facts of historic and recent mass atrocities and developing a policy framework for prevention and response to mass atrocities.[14] The study directive is similar to a koan: You know what the response to mass atrocities looks like. What does the prevention of mass atrocities look like?

A. Triggering Factors

The U.S. Army Peacekeeping and Stability Operations Institute[15] created the MAPRO Handbook to answer the *koan*

[hereinafter MAPRO HANDBOOK], https://www.pksoi.org/document_repository/doc_lib/MAPRO_Policy_Handbook_(6-Mar-2012).pdf.

[10] *See generally id.*

[11] *See id.* at 1-2.

[12] *Id.*

[13] Directive on Creation of an Interagency Atrocities Prevention Board and Corresponding Interagency Review, 2011 DAILY COMP. PRES. DOC. 259 (Aug. 4, 2011), https://www.gpo.gov/fdsys/pkg/DCPD-201100549/pdf/DCPD-201100549.pdf.

[14] *Id.*

[15] *Background & History*, PEACEKEEPING & STABILITY OPERATIONS INST., http://pksoi.armywarcollege.edu/index.cfm/who-we-are/background-history/ (last visited Apr. 19, 2017); *See also* Robert Bunker, *New Website Launch: US Army Peacekeeping and Stability Operations Institute,* SMALL WARS J. (March

posed by the Presidential Study Directive.[16] The Handbook says, "[i]t is better to prevent mass atrocities than to have to respond, as prevention implies that widespread violence does not occur."[17] The Handbook then details potential warning signs, triggers, and processes that could lead to mass atrocities.[18] The Handbook lists potential factors that heighten the likelihood of atrocities occurring in target areas.[19] It prioritizes monitoring states with ongoing-armed conflict, civil unrest, or dramatic regime changes.[20] The Handbook directs analysts to pay particular attention to the following six triggering factors: (1) closed societies; (2) with histories of atrocities; (3) that currently have weak, unstable, or poor leadership; (4) perpetuating impunity for previous perpetrators; (5) preventing institutional accountability and peaceful resolution; and (6) allowing continued discrimination.[21] The Handbook notes that even in circumstances presenting these warning signs, leaders lobbying for mass atrocities cannot conduct mass atrocities without motive, means, and opportunity:

> [P]erpetrators require the motivation, means, and opportunity to conduct mass atrocities. Motivations may include identity issues, the desire to acquire political or economic power, territory, or revenge. Additionally, motivations are probably strongest when perpetrators desire not to lose power they already have. Means includes the political latitude, plans, and the supporters required to commit the mass atrocities. The opportunity to commit mass atrocities generally occurs during three stages: a

15, 2016, 9:48 AM), http://smallwarsjournal.com/blog/new-website-launch-us-army-peacekeeping-and-stability-operations-institute.

[16] MAPRO HANDBOOK, *supra* note 9, at 1.

[17] *Id.* at 17. In typical government reasoning, the focus is not on the sanctity of human life but rather on effective resource management. *Id.*

[18] *Id.* at 12-13.

[19] *Id.*

[20] GENOCIDE PREVENTION TASK FORCE, PREVENTING GENOCIDE: A BLUEPRINT FOR U.S. POLICYMAKERS 24 (2008), http://www.ushmm.org/m/pdfs/20081124-genocide-prevention-report.pdf [Hereinafter PREVENTING GENOCIDE] ("Virtually all instances of genocide or mass atrocities since World War II occurred coincident with or closely following a major internal conflict or the taking of power by more radical or more harshly authoritarian leaders.").

[21] MAPRO HANDBOOK, *supra* note 9, at 13.

> *crisis* that triggers the events, perpetrator *mobilization* to conduct mass atrocities, and *violence* which may begin at a low level before escalating to mass atrocities.[22]

Both Rwanda and Bosnia fit this model by displaying the indicative factors and then providing the motive, means, and opportunity for mass atrocities to occur. Rwanda's lack of technology created a closed society.[23] It had ineffective and self-protecting leadership that allowed continued discrimination and perpetuated impunity for those who previously persecuted its Tutsi[24] citizens.[25] In addition, Rwanda's Hutu-dominated[26] government did not allow the Tutsi citizens to peacefully demand accountability for that persecution.[27] The preliminary success of the Rwandan Patriotic Front[28] and resulting Arusha accords[29] caused Hutu leaders to fear retribution by the Tutsi for the years of discrimination and persecution, thereby providing adequate motivation for the Hutu to cleanse themselves of potential Tutsi rivals.[30]

When it was part of Yugoslavia, Bosnia had almost none of the indicative factors. It was an open society with an established and functioning government.[31] Yugoslavia's leader, Josip Broz Tito,[32] enforced a policy of "Brotherhood and Unity" that served as the glue that held the united Yugoslavia's diverse ethnicities together.[33] With the death of Tito, however, the glue disintegrated

---

[22] *Id.*
[23] SAMANTHA POWER, A PROBLEM FROM HELL: AMERICA AND THE AGE OF GENOCIDE 336-37 (2013).
[24] A minority ethnic group in Rwanda. *Id.*
[25] *Id.*
[26] The majority ethnic group in Rwanda. *Id.*
[27] *Id.*
[28] An armed rebel group composed of Tutsi soldiers that returned from Uganda to battle the government of Rwandan for persecuting other Tutsi citizens. *Id.*
[29] The peace agreement signed to end the Rwandan Civil War. *Id.*
[30] *Id.*
[31] ELIZABETH NEUFFER, THE KEY TO MY NEIGHBOR'S HOUSE: SEEKING JUSTICE IN BOSNIA AND RWANDA 18 (2003).
[32] Josip Broz Tito led Yugoslavia in a variety of rolls from 1939 until his death in 1980. *Id.*
[33] *Id.*

and ethnic tension as well as economic crisis left Yugoslavia in shambles.[34] The ethnically divided nations that emerged from the collapse of Yugoslavia generally portrayed the majority of the indicative factors.[35] The rise of Slobodan Milosevic[36] to a leadership position among Serb nationalists and his desire to establish a separate, homogeneous "greater Serbia" provided motivation for the ensuing ethnic cleansing.[37]

Once both countries displayed enough factors to generate an extremely high risk that mass atrocity would occur, they then also provided means, motive, and opportunity for the atrocities to occur. As to means, both incidents occurred during periods of conflict, generating easy access to organized planning and support units from established military forces.[38] Then, civil war provided the triggering crises and violence that mobilized military and paramilitary perpetrators of atrocities.[39]

B. MAPRO's Signs and Indicators on the Road to Mass Atrocity

The Handbook suggests that if countries display the indicative factors and provide motive, means, and opportunity, analysts should examine the progression of the institutional drive towards mass atrocity to provide an assessment of whether prevention of, or response to, mass atrocity would be appropriate.[40] The Handbook details eight institutional stages that generally lead to mass atrocities: (1) classification; (2) symbolization; (3) dehumanization; (4) organization; (5) polarization; (6) preparation; (7) extermination; and (8) denial.[41]

---

[34] *Id.* at 7-8.
[35] *Id.* at 24.
[36] The former President of Serbia and of Yugoslavia. *Id.*
[37] *Id.*; *see also* POWER, *supra* note 23, at 247-49.
[38] *See* POWER, *supra* note 23, at 336-37 & 247-49.
[39] *Id.*.
[40] MAPRO HANDBOOK, *supra* note 9, at 13.
[41] *Id.* at 13-16 (citing Gregory H. Stanton, *The 8 Stages of Genocide*, GENOCIDE WATCH (1998), http://www.genocidewatch.org/aboutgenocide/8stagesofgenocide.html); *see also Preventing Genocide*, *supra* note 23, at 19 (urging caution because mass atrocities "have unfolded differently in each case.").

The classic example (and likely the basis for the model) of these indicators is the Jewish Holocaust. By incorporating the Losener proposal[42] into the First Regulation to the Reich Citizenship Law, which categorized the levels of non-Aryans,[43] and by passing the Law for Protection of German Blood and Honor, which prohibited marriages and extramarital relations between Jews and Germans,[44] Germany completed the classification stage. It demonstrated symbolization when it passed laws requiring Jews to wear badges depicting the Star of David.[45] When Hitler spoke to the *Reichstag*[46] as the leader of Germany and named the Jews as the cause of the world's problems,[47] it was another part of the German government's propaganda machine that worked to dehumanize the Jews in the eyes of the German citizens.[48] Germany organized its *Schutzstaffel* (SS)[49] and instituted logistics channels for future extermination operations,[50] thereby completing the organization stage. By officially discriminating against Jews living, working, or commuting with Aryans,[51] Germany executed the polarization stage. Ghettoization is part of the definition of the preparation stage because it allows perpetrators to easily prepare potential victims for forced relocation and extermination.[52] Germany, therefore, completed this

[42] Losener proposed defining a Jew very precisely in a hierarchical manner in order to address the dangers of decreasing the purity of German bloodlines through mixed marriages with Jews. GERALD E. MARKLE, MEDITATIONS OF A HOLOCAUST TRAVELER 78-79 (1995).

[43] RAUL HILBERG, THE DESTRUCTION OF THE EUROPEAN JEWS 31 (1985).

[44] *Id.* at 42.

[45] *Id.* at 58.

[46] The Parliament of the Third Reich. HILBERG, *supra* note 43, at 13.

[47] *Id.*; *see also* Holocaust Educ. & Res. Team, *Hitler Speaks to the Reichstag on the Jewish Question*, HOLOGUSTRESEARCHPROGJECT.ORG, http://www.holocaustresearchproject.org/holoprelude/jewishquestion.html (last vistited Feb. 18, 2017) ("If the international Jewish financiers in and outside Europe should succeed in plunging the nations once more into a world war, then the result will not be the bolshevization of the earth, and this the victory of Jewry, but the annihilation of the Jewish race in Europe!").

[48] *See generally* KEITH SOMERVILLE, RADIO PROPAGANDA AND THE BROADCASTING OF HATRED: HISTORICAL DEVELOPMENT AND DEFINITIONS 142 (2012).

[49] The paramilitary forces of the Nazi Regime known for their brutality. HILBERG, *supra* note 43, at 53.

[50] *Id.*

[51] *Id.* at 48-49, 53-56.

[52] MAPRO HANDBOOK, *supra* note 9, at 15-16.

stage when it relocated all its Jews to ghettos.[53] German concentration camps and the mobile killing teams, *Einsatzgruppen*,[54] were part of Germany's extermination stage. Finally, Germany rounded out the stages of mass atrocity by completing the denial stage when government officials used excuses of "labor" and "resettlement" to hide the true meaning of the Final Solution.[55]

This Paper does not focus its criticism on these factors, triggers, and indicators. Instead, it is directed at the model of prevention that uses these assessment tools. The assessment tools presented in the Handbook provide a well-rounded foundation for future analysts.[56] In actual assessments, however, analysts should use more than one assessment toolkit, as not all mass atrocities display the same progression or violence in their progression.[57] In fact, the Stanley Foundation retroactively conducted a study of countries in 1997 with similar triggering factors to the six triggering factors listed in the Handbook and compared their predictions to the actual occurrence of atrocities.[58] The results of the study showed a forty-seven percent chance of accurately predicting whether an atrocity would occur in the target country.[59] The Handbook provides a starting point for analysis, but there is no "one size fits all" assessment toolkit for determining the likelihood of mass atrocities, and there is not a set, linear process to prevent all predicted mass atrocities.

---

[53] HILBERG, *supra* note 43, at 81-86 (detailing the logistics and process of ghettoization before extermination).
[54] *Id.* at 102.
[55] The Nazis used the code words "Final Solution" to describe their efforts at destroying the Jews as a whole—their answer to the "Jewish Problem." POWER, *supra* note 23, at 34.
[56] *See generally* MAPRO HANDBOOK, *supra* note 9.
[57] PREVENTING GENOCIDE, *supra* note 20, at 19 ("For example, forced exile of Armenians into unlivable conditions, slave labor and starvation in Cambodia's 'killing fields,' and attacks by paramilitary death squads in Guatemala.").
[58] Alex J. Bellamy, *Mass Atrocities and Armed Conflicts: Links, Distinctions, and Implications for the Responsibility to Prevent*, THE STANLEY FOUND. (Feb. 2011), http://www.stanleyfoundation.org/publications/pab/bellamypab22011.pdf.
[59] *Id.*

III. THE MAPRO'S SIX-STEP LOGICAL/"IF-THEN" PROCESS TO SOLVING THE PARADOX

The Handbook attempts to solve a paradox by applying logical reasoning.[60] The MAPRO model proposes a six-step linear process for preventing mass atrocities: (1) Routine Monitoring and Engagement; (2) Problem Identification and Initial Guidance; (3) Situation Analysis and Assessment; (4) Policy Formation; (5) Plan Development; and (6) Execution.[61]

A. Routine Monitoring and Engagement

In the "Routine Monitoring and Engagement" step, the Handbook encourages agencies in and outside the region currently being monitored for potential mass atrocities to "incorporate a 'MAPRO' lens[62] as they [sic] conduct their activities and assessments and promote U.S. national interests."[63] The Handbook suggests that if organizations shift their perception of their environment to a MAPRO lens while conducting their steady state operations, it "will help identify problematic situations as they develop, and potentially diminish the likelihood that mass atrocities will occur."[64] This suggestion implies that organizations (a) understand what a MAPRO lens is and (b) have the resources and ability to shift their day-to-day approach to operations and reporting. It also assumes entities pinpointed for responsibility care about U.S. national interests. If the agencies and organizations on the ground cannot adopt the MAPRO lens or U.S. national interests, the rest of the recommended process stalls.

B. Problem Identification and Initial Guidance

The Handbook's next step, "Problem Identification and Initial Guidance," emphasizes that American embassies will play a key role in identifying possible emerging crises to interagency

---

[60] MAPRO HANDBOOK, *supra* note 9, at 34.
[61] *Id.*
[62] *Id.* at 61 (defining the MAPRO lens) ("[T]he institutional ability to observe and orient on developments that could presage mass atrocities and take early action to mitigate them.").
[63] *Id.* at 34.
[64] *Id.*

planning teams.[65] But the same organizations that should be adopting the MAPRO lens in the prior step (non-government organizations, the United Nations, media, or allies) should also provide their input.[66] This reliance on problem identification by embassies also presents a problem. In historic mass atrocities, ambassadors have either been misled (as was the case of Germany and Bosnia)[67] or ignored (as was the case in the Armenian genocide).[68] If the problem cannot be identified because those agencies with input are not focused on the specific problem or their spokespersons are misled or ignored, the problem cannot be prevented.

After relying on underfunded agencies and organizations to help identify when the planning process should start, the Handbook then places an inordinate responsibility on interagency planning teams to complete the rest of the planning process.[69] The model proposes an interagency planning team with vague, ever-changing input and guidance, consisting of members from varied, inherently political agencies.[70] The model then suggests this team, even with all its impediments, can function effectively and accomplish its mission: coming to an agreement on the analysis of the data presented to them and producing a single, agreed upon policy and subsequent plan of action.[71] A team may coalesce if the planning authority chooses an experienced, confident leader to head the interagency planning team, but such appointments can easily fall along political lines instead of meritorious ones. Without efficient leadership, planning teams require extensive training and experience before they can efficiently, effectively, and successfully complete such a mission. Most likely, when the MAPRO method is utilized, none of the teams will have any real life training *as a team*. The lack of training, the inherent impediments of the

---

[65] *Id.* at 35.

[66] *Id.*

[67] POWER, s*upra* note 23, at 260 (noting that ambassadors and diplomats "bring a gentlemen's bias to diplomacy" that allows them to be easily persuaded by charismatic individuals like Hitler and Milosevic).

[68] *Id.*

[69] MAPRO HANDBOOK, *supra* note 9, at 28.

[70] *Id.* at 28-31; *see id.* at 35 ("Whether a planning effort occurs, and how much effort is devoted to it, will depend [on] the relative assessment of risk and other competing priorities.").

[71] *Id.* at 35.

previous steps, and the difficulty of the Handbook's mission for the team makes the team's mission success improbable—and prevention impossible.

C. Situational Analysis and Assessment

The interagency planning team begins its arduous mission in the third step, "Situation Analysis and Assessment."[72] The interagency planning team compiles all the information gathered by local embassies, local non-governmental agencies, and other organizations, and then assesses and analyzes all of the complex interactions in the society.[73] The Handbook also relies heavily on the interagency planning team while noting, "an [interagency planning team] can expect that the guidance and parameters may be vague, uncertain, and frequently changing due to the complexity of dynamic political change in the international environment."[74] The Handbook also mentions that an accurate assessment "can take up to a year to plan, research and develop."[75]

D. Policy Formation

Once the interagency planning team analyzes the situation and assesses the likelihood of the occurrence of a mass atrocity, it executes the fourth step of "Policy Formation" and forms a policy and strategic plan to present, in memo format, to the President or Principals Committee.[76] In addition to accurately predicting the likelihood of mass atrocity and characterizing the U.S. interest in preventing that specific occurrence, the planning team must consider the available resources in its policy formation because "[a] policy that is too ambitious for the level of political will and available resources will inevitably prove unsuccessful and do a disservice to the victims and to the [United States] by inflating expectations and engendering unnecessary opposition . . . ."[77]

---

[72] MAPRO HANDBOOK, *supra* note 9, at 38.
[73] *Id.* at 41-52.
[74] *Id.* at 37.
[75] *Id.* at 39.
[76] *Id.* at 52.
[77] *Id.* at 55.

E. Plan Development

After approval at the policy and strategic level, the fifth step "Plan Development" directs "parallel planning efforts . . . by Departments in Washington and field organizations . . ."[78] in order to develop the specific prevention plan for a target society or situation.[79] The specific plan depends on how imminent a mass atrocity seems.[80] Any student of strategic plans can tell you that it is difficult to translate strategic guidance into an operational plan.[81]

F. Execution

Effective translation from strategic guidance to an operational plan is required to complete the sixth and final step: "Execution."[82] The plan developed for the individual location and the progression of the impending mass atrocity must be communicated accurately to the units and agencies on-site for precise execution with efficient feedback and reporting to the interagency planning team for continued monitoring and assessment of the situation.[83] The method for planning prevention operations proposed in the MAPRO supposes that aid workers, officials, or agents on the ground can effectively communicate to policy makers and planning teams throughout the process so that changes to the policy, plan, and execution can be implemented.[84] While communications technology has increased the fluidity of responsiveness, it can also create knowledge management[85]

---

[78] *Id.* at 57.

[79] *See id.* at 58.

[80] *Id.* at 61-62.

[81] JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, Joint Operation Planning III-3 (Aug. 11, 2011). Understanding the operational environment, defining the problem, devising a sound approach, and developing a workable solution are rarely achieved the first time. Strategic guidance addressing complex problems can initially be vague, requiring the commander to interpret and filter it for the staff. *Id.*

[82] *See* MAPRO HANDBOOK, *supra* note 9, at 67.

[83] *Id.* ("Successful execution requires effective coordination among agencies in Washington and the field, as well as accurate and timely assessment consisting of monitoring, evaluation, and decision-making.").

[84] *Id.*

[85] *Michael E.D. Koenig, What is KM? Knowledge Management Explained*, KMWORLD (May 4, 2012), http://www.kmworld.com/Articles/Editorial/What-Is-.../What-is-KM-Knowledge-Management-Explained-82405.aspx.

problems.[86] Even if the interagency planning team could get experts in every interacting field of study at the location of a predicted mass atrocity, the interagency planning team would then need to catalog and process all the data supplied by the experts. With limited resources, the planning team would then face issues of restrictions on information sharing and challenges with the interoperability of information sharing systems.[87] The fact that the Handbook specifically tells analysts to ignore broader trends[88] significantly decreases the chances that one interagency planning team could effectively deconstruct and identify the complex factors contributing to the impending atrocity. To then ask the same interagency planning team to pinpoint a single course of action for policy formation to prevent the atrocity seems absurd.

Even if the planning team could develop a course of action for prevention, as noted by a complexity scholar, "[c]ommand-and-control methods, detailed forecasts and plans are effective only for linear systems and fail to achieve desired outcomes in complex environments that involve vast numbers of interactions where the results cannot be traced to specific causes."[89] These complex environments have vast economic, social, and political interactions setting the conditions for mass atrocity.[90] Most agencies do not have the moxie to catalyze economic, social, and political change quickly enough to derail an institutionalized drive toward mass atrocity.[91] Stopping and bringing to justice one leader may slow the momentum, but to prevent mass atrocity or its recurrence, the unlucky interagency planning team and organizations in the field must consider the intricate connections in these complex environments and precisely dictate the policies, plans, and operations that will "fix" a society in order to prevent a mass atrocity.

---

[86] PREVENTING GENOCIDE, *supra* note 20, at 21-22.
[87] *Id.*
[88] MAPRO HANDBOOK, *supra* note 9, at 39 ("In nearly every case, it is important to understand the specifics regarding local actors and dynamics, as broader generalizations can be misleading.").
[89] Serge Loode, *Peacebuilding in Complex Social Systems*, 18 J. PEACE CONFLICT & DEV. 68, 73 (Dec. 2011) (footnote omitted) (citing another source).
[90] *Id.* at 70 ("Complex social systems can be found in markets, families and villages. What these systems have in common is that they cannot be understood and manipulated by reducing them to their individual components.").
[91] *Preventing Genocide*, *supra* note 20, at 37-53.

The prevention proposed in the Handbook is too linear and dependent on logical action and reaction.[92] While the proposed "if-then" method may seem logical and easily executed at the policy and front line levels, that same linear thinking dooms any chance at effective prevention.[93] Societies should not be analyzed linearly.[94] The simple interaction of two people, for instance an Archduke and a young Serb, can have international and catastrophic results.[95] Multinational and interagency attempts to prevent mass atrocities and genocide involve far more agents and their independent and interdependent social relationships, underlying motivations, and timelines for action.[96] A map of the impacts of a single prevention meeting more resembles a spider web than a linear progression. Complex systems like the societies at risk for mass atrocities simply do not follow Newtonian-like laws of nature.[97] Instead,

---

[92] *See* Diane Hendrick, *Complexity Theory and Conflict Transformation: An Exploration of Potential Implications* 59 (U. of Bradford Ctr. for Conflict Resol. Dep't of Peace Stud., Working Paper No. 17, 2009); *see also* Loode, *supra* note 89, at 73 ("Peacebuilders are well advised not to rely too much on logical frameworks and project plans and to be able to change or abort projects.").

[93] *See* Loode, *supra* note 89, at 81 ("Contemporary peacebuilding practice is still governed by a positivist, reductionist and linear understanding of social change. This leads to the assumption that programme and project outcomes can be predicted and planned with certainty. In complex social systems such planning is impossible.").

[94] *Id.* at 72-73.

[95] In 1914, a young Serb nationalist assassinated Archduke Franz Ferdinand, heir to the Austro-Hungarian empire, arguably instigating World War I. *1914 Archduke Ferdinand Assassinated*, HISTORY.COM, http://www.history.com/this-day-in-history/archduke-ferdinand-assassinated (last visited April 5, 2017).

[96] JOHN PAUL LEDERACH, THE MORAL IMAGINATION: THE ART AND SOUL OF BUILDING PEACE 33 (2005); *see also* Loode, *supra* note 89, at 72 ("One of the observations about complex systems is that system effects are non-linear and unpredictable, because they emerge from the large numbers of interactions in the network of agents.").

[97] The only exception might be the second law of thermodynamics: Closed systems will have escalating entropy or chaos. Glenn Research Ctr, *The Second Law of Thermodynamics*, NASA, https://www.grc.nasa.gov/www/k-12/airplane/thermo2.html (last updated May 5, 2015). This law presumes that systems will continue to grow in complexity over time. *Id.* In general, however, it only applies to closed systems, which are isolated from interactions with any other systems. *2nd Law of Thermodynamics*, CHEMISTRY LIBRETEXTS, http://chem.libretexts.org/Core/Physical_and_Theoretical_Chemistry/Thermodynamics/Laws_of_Thermodynamics/Second_Law_of_Thermodynamics (last updated Nov. 5, 2016). In addition, it does not provide an avenue for containing

their "multiplicity, interdependency, and simultaneity"[98] are better described by the laws of subatomic and quantum systems.

IV. THE UNCERTAINTY PRINCIPLE AND THE QUANTUM NATURE OF MASS ATROCITIES

The developers of the Handbook attempted to apply logic to the discussion and deconstruction of mass atrocities. A more holistic approach to solving the problem would have revealed to the Handbook developers the negative implications the Heisenberg uncertainty principle has on their model. According to the Heisenberg uncertainty principle, formulated by Werner Heisenberg in 1927, it is impossible to determine the momentum and position of a particle of light (photon) simultaneously.[99] The more advanced explanations of the uncertainty principle revolve around the idea that photons exist as waves and particles in numerous, uncertain states until they are observed.[100] By integrating the possible wave functions for a photon, an observer collapses all the possible wave functions into one wave function to determine the specific momentum.[101] Due to the nature of wave functions, this collapsed wave function provides a specific speed and direction but makes position impossible to determine.[102]

At its most basic level, the Heisenberg uncertainty principle states that the act of observing a photon changes basic elements of

---

or reacting to the increased complexity. *Id.* It simply states the system will become more complex. *Id.*

[98] LEDERACH, *supra* note 96, at 33.

[99] CAPRA, *supra* note 1, at 140.

[100] David Cassidy, *The Uncertainty Principle*, AM. INST. OF PHYSICS, https://www.aip.org/history/heisenberg/p08.htm (last visited Feb. 16, 2016). The Schrödinger's cat thought experiment is helpful in understanding the numerous states of the uncertainty principle. Schrödinger imagined placing a cat in a lead box with radioactive material. *Uncertainty Principle*, UNIV. OF OR., http://abyss.uoregon.edu/~js/21st_century_science/lectures/lec14.html (last visited Feb. 16, 2016). By opening the box, the observer collapsed all other possibilities. However, until someone opened the box to observe whether the cat was alive or dead, it was both dead and alive. *Id.*

[101] *Uncertainty Principle*, GA. ST. UNIV., http://hyperphysics.phy-astr.gsu.edu/hbase/uncer.html (last visited Feb. 16, 2016).

[102] *Id.*

the speed and trajectory of the photon.[103] In order to study a photon, an observer must bounce light off it (much like your eyes pick up on the light bouncing off of these letters to enable you to read them).[104] The instrumental light and the desired photon bounce off each other like billiard balls, altering the momentum and therefore the velocity of the desired photon.[105] Thus, whether integrating or observing a photon, scientists can choose to know where a particle was when they chose to observe it but not know how quickly it is going after adding the momentum of the instrumental photon, or they can choose to know how quickly and where a particle was going but, due to its high speed and resulting deflection, have no idea where the particle is after they measure its velocity.[106]

The institutionalized drive to mass atrocities is similar to a subatomic particle, making it impossible to determine its position and trajectory at the same time; for example, once the Serbs discovered international agencies were capturing satellite images of mass graves (an indicator of where an institution falls in the spectrum of mass atrocities) in Bosnia and Herzegovina, the Serbs reformed their institutional policies on mass killings and mass graves—making it impossible to determine how quickly they were progressing to an all-out genocide.[107] There, much like light in particle physics labs, the act of observation changed the course and speed of the subject of observation.

Mass atrocities also demonstrate the same nature as light because of their various forms and ever-changing possibility of occurrence. It is difficult to gather information on mass atrocities that is distinguishable from other events in the area.[108] Embassies—which would be best equipped to provide policy makers with up-to-date, frontline information—make this issue more complicated as they generally focus on activity in the capital, not in rural areas where many of the most recent mass atrocities have occurred.[109] Analysts on the ground may have many reports

[103] CAPRA, *supra* note 1, at 141.
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] POWER, *supra* note 23, at 247-49.
[108] *Preventing Genocide*, *supra* note 20, at 17 & 19.
[109] *Preventing Genocide*, *supra* note 20, at 20.

from rural areas about increased violence but would be generally unable "to distinguish systematic killing of civilians from more generalized background violence as most if not all mass atrocities occur in the context of a larger conflict or a campaign of state repression."[110] In accordance with Heisenberg's uncertainty principle, analysts could only discuss the frequency of violence but not where the violence placed the area on the spectrum of mass atrocities.

V. THE UNCERTAINTY PRINCIPLE'S NEGATIVE IMPACT ON THE MAPRO'S RECOMMENDED PROCESS

The Handbook falls victim to the Heisenberg uncertainty principle when it suggests to alter actions in areas with predicted mass atrocities. As part of the "Plan Development" step, the Handbook proposes planning reaction operations to use at each stage as the likelihood of mass atrocity increases.[111] If a situation moves from unlikely to have mass atrocities to likely to have mass atrocities, the Handbook suggests implementing efforts to decrease violence by "addressing grievances," "supporting legitimate and effective governance," and "protecting minority rights."[112] These recommended efforts are analogous to the instrumental photons in that they may tell the prevention forces how rapidly the situation is developing into mass atrocity or where in the spectrum the country has been, but impedes further assessments. Further assessments would be impeded because simply addressing grievances alerts those driving the institution toward mass atrocity that the United States is observing their actions and could intervene. Generally, a perpetrator's knowledge that they are under surveillance causes perpetrators to alter their tactics.[113] Thus, even if an interagency

---

[110] *Id.* at 21.

[111] MAPRO HANDBOOK, *supra* note 9, at 61.

[112] *Id.* at 62.

[113] Generally, a perpetrating group's knowledge that they are under surveillance causes perpetrators to cease the perpetration of the crime or alter their tactics. *See* Adrienne Isnard, *Can Surveillance Cameras be Successful in Preventing Crime and Controlling Anti-Social Behaviours?*, AUSTRALIAN INST. OF CRIMINOLOGY 1 (Aug. 2-3, 2001), http://www.aic.gov.au/media_library/conferences/regional/isnard1.pdf; *see also* A.R. Gillis, *Crime and Surveillance in Nineteenth-Century France*, 95 AM. J. SOC. 307 (1989).

planning team continuously monitors and assesses the situation, prevention will still be impeded because the analysis and assessment tools will likely effectuate a change in the overall situation, causing the planning team to restart their process.

The third phase of the "Plan Development" step increases the chances that U.S. observation will interfere with an interagency planning team's ability to continuously assess the likelihood of mass atrocity. When the likelihood of mass atrocity increases from *likely to occur* to *imminent risk of mass atrocity*, the Handbook recommends "diplomatic, legal, economic, [and] financial . . ." tools that "punish, isolate, undermine, intimidate, or apply significant pressure to coerce perpetrators" and the limited use of military intervention.[114] Much like two particles of light interacting, these recommendations may affect the institutionalized drive to mass atrocity but only to shift one course of action to another with a different timeline for execution.

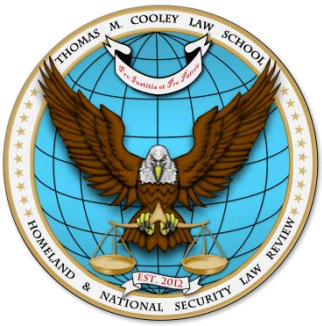
As the United States acts in accordance with the Handbook and increases its observation, inquiries, and presence, the motivation, means, and opportunities of the local leadership may change, but their ideology likely will not. Instead, as was the case in Serbia, those in power will likely react to the U.S. intervention by accelerating the mass atrocity timeline or by regrouping and attempting another avenue to achieve their goals. This reaction, in a society on the road to mass atrocity, creates self-inflicted impediments to the prevention planning process because, as the Handbook recommends, "[w]hen the overall situation has changed significantly, it may be necessary to take a fresh comprehensive look in order to develop a new plan."[115] A "fresh look" would essentially require restarting the MAPRO policy planning process.[116] As discussed above, the assessment step can take nearly a year.[117] The Rwandan genocide saw 800,000 killed in 100 days.[118] The ever-changing, intricately connected nature of the

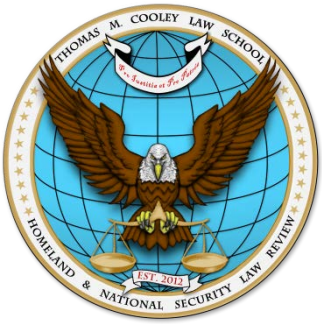
[114] *Id.* at 70.
[115] *Id.* at 52.
[116] *Id.*
[117] *Id.* at 39 ("A thorough [Interagency Conflict Assessment Framework] can take up to a year to plan, research and develop.").
[118] POWER, *supra* note 23, at 334.

drive to mass atrocities does not lend itself to the time-consuming, linear process set forth in the MAPRO Handbook.

VI. CONCLUSION

The system proposed in the Handbook will not prevent mass atrocities. The writers and developers of the Handbook attempted to use language and logic to solve the paradox of mass atrocities and their prevention. After reading the Handbook, a Zen Buddhist master would likely pose the *koan* again, "You clearly know how to respond to mass atrocities. How do you prevent one?" The Handbook would likely serve as a solid foundation for future endeavors to develop assessment tools, but its linear approach to preventing mass atrocities creates self-impeding feedback loops; however, this should not be considered a failure. Instead, the Zen Buddhist master would likely congratulate the writers and developers of the Handbook on learning the first lesson in understanding the problem: The paradox of prevention cannot be resolved through logical, "if-then" analysis and systems. He would remind the United States and its partner agents that to properly understand the problem (and therefore more easily solve it), they should adopt a holistic approach to thinking about the problem or shift the nature of how they operate. What those shifts look like is beyond the scope of this Paper but should be a primary consideration as the United States refines its policies on prevention.


THOMAS M. COOLEY LAW SCHOOL
Ex Scientia et Fac Fortis
HOMELAND & NATIONAL SECURITY LAW REVIEW
EST. 2012



CYBER FORCE IN AN ANA[LAW]G WORLD: ON SELF-DEFENSE, CYBER OPERATIONS, AND THE UNITED STATES LAW OF WAR MANUAL

Stefan Ducich

I. INTRODUCTION

In June 2015, the Department of Defense (DoD) issued its Law of War Manual (DoD Manual) as a department-wide "resource for DoD personnel . . . on the law of war"—the first such consolidated manual in nearly six decades.[1] The DoD Manual is largely a restatement of previously posited legal and policy positions taken by the United States regarding its current treaty obligations; and in this regard, the substantive content of the DoD Manual is not particularly innovative.[2] For the first time, the DoD Manual includes a Cyber Operations chapter.[3] This chapter

[1] OFF. OF GEN. COUNS. DEP'T OF DEF, U.S. DEP'T OF DEF. LAW OF WAR MANUAL, iii (2016), [hereinafter LAW OF WAR MANUAL] http://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf.

[2] David Glazier, *The DoD Law of War Manual: What is it Good For?*, JUST SECURITY (July 28, 2015, 10:19 AM), https://www.justsecurity.org/24977/dod-law-war-manual-good-for (dicussing that the previous DoD Manual dated to 1956, with a single amendment in 1976; thus, that manual lacked guidance on influential domestic and international legal developments from the last half-century).

[3] The DoD Manual contains nineteen chapters and a total of 1,166 pages. *See generally* LAW OF WAR MANUAL, *supra* note 1. *See also* Charlie Dunlap, *Cyber Operations and the New Defense Department Law of War Manual: Initial*

reiterates the DoD's position that cyberspace represents a domain of warfare[4] and that the United States is bound by the rules of international law in the conduct of any action falling within that domain.[5]

In international law, specific thresholds define a State's ability to respond to applicable gradations of impermissible force, up to and including the inherent right of a State to respond in self-defense to an armed attack.[6] This customary norm is most clearly delineated in the International Court of Justice's (ICJ) 1986 decision, *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua)*.[7] However, the United States rejected both the jurisdiction of the ICJ to adjudicate the merits of that case as well as the resulting analysis of threshold distinctions.[8] Instead, based on its interpretation of customary international law, the United States asserted a right to respond proportionally in self-defense, regardless of the gravity of the force incurred.[9] The DoD

Impressions, LAWFARE (June 15, 2015, 3:00 PM), https://lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions (noting that Cyber Operations, Chapter XVI, contains only fifteen pages, though it represents an evolution in DoD transparency about cyber as an operational domain).

[4] *See* LAW OF WAR MANUAL, *supra* note 1, at 986 ("As a doctrinal matter, DoD has recognized cyberspace as an operational domain in which the armed forces must be able to defend and operate, just like the land, sea, air, and space domains.").

[5] "Specific law of war rules may apply to cyber operations" and where no direct rule governs "law of war principles provide a general guide for conduct during cyber operations in armed conflict." *Id.* at 987.

[6] *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

[7] *Id.*

[8] *Id.* para. 10.

[9] In 1988, then-Legal Advisor for the Department of State, Abraham Sofaer, clarified the U.S. position regarding precipitating acts that trigger responsive force: the United States reserves the right to respond to acts of violent aggression, pursuant to necessity and proportionality. Abraham D. Sofaer, *Joint Luncheon with the Section of International Law and Practice of the American Bar Association*, 82 AM. SOC'Y INT'L L. PROC. 420, 421–22 (1988) ("The inherent right of self-defense potentially applies against any illegal use of force and . . . the term 'armed attack' should be defined to include forms of aggression historically regarded as justifying resort to defensive measures."); s*ee also* William H. Taft, IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE J. INT'L L. 295, 300 (2004) (arguing that proportionality restricts the scope of

Manual generally asserts this position and indeed explicitly notes that the United States may potentially respond self-defensively to "any illegal use of force," including within the cyber context.[10] Thus, rather than being bound by explicit thresholds, as with the framework set out in *Nicaragua*, the United States maintains that its potential response is bound only by internal determinations of proportionality and necessity.[11]

Generally, collapsing the distinction between an impermissible use of force and an armed attack may be in conflict with international law;[12] however, the current legal ambiguities within the cyber context further exacerbate the issue.[13] To that end, the DoD Manual's non-distinction, as it pertains to cyber operations, likely amounts to a violation of the United Nations (U.N.) Charter (Charter) as well as the customary rule of proportionality in international law.[14] Such a position improperly bypasses the U.N. Security Council (Security Council) and its exclusive power to check a State's response to actions below the "armed attack" threshold.[15] Moreover, should the United States

response, but the gravity is irrelevant "to determining whether there is a right of self-defense in the first instance.").

[10] *See* LAW OF WAR MANUAL, *supra* note 1, at 991.

[11] *Id*. ("Any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.").

[12] Since the United States has maintained the position that it may respond in self-defense to any illegal use of force directed against it since at least 1988, one may argue that it has persistently objected to the threshold analysis and so is not bound by customary international law in this regard. *Cf.* Sofaer, *supra* note 9. Article 38 of the ICJ Statute defines customary law as any "general practice accepted as law." Statute of the International Court of Justice. art. 38, http://www.icj-cij.org/documents/?p1=4&p2=2. Proving the existence of such a norm requires the coexistence of State practice, as well as a belief that adherence to the norm is borne out of a sense of legal obligation, or *opinio juris (sive necessitates)*. Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 572 (2011). Despite U.S. rejection of the ICJ severity analysis, the overarching customary prohibition on force governs all States. *Cf. id.*

[13] *See* discussion *infra* Section III.A.2 (evaluating the dangerous effects of overly permissive terms in an ill-defined legal context).

[14] *See infra* Part III (analyzing U.S. obligations in the application of its Cyber Operations policy).

[15] *See infra* text accompanying notes 29, 106 (arguing that the U.N. Charter builds a legal architecture vesting limited but exclusive sovereignty over lawful force in the U.N. Security Council).

resort to self-defensive action in response to "any illegal use of force," as broadly defined by the DoD Manual, such action may constitute a violation of *jus ad bellum* proportionality.[16] Finally, if the United States responds to a substantially low-level cyber event with force, such an action may constitute a forceful reprisal, or a violation of *jus in bello* proportionality.[17]

Part II assesses the relationship of the normative legal framework to the cyber context, regarding traditional Charter-based law and customary legal norms as well as the legal position of the United States. Part III argues that the ambiguity in legal definitions—and concomitant thresholds for responsive action vis-à-vis cyber operations—complicates the U.S. position that it may respond in self-defense to any illegal use of force. Such per se responsive action violates Articles 2(4), 24, 39, and 51 of the U.N. Charter as well as the principles of proportionality in customary international law—both in the resort to force and in the execution of a potentially forceful reprisal.

Next, Part IV offers a two-fold recommendation to bring U.S. policy into compliance with international legal norms. On the domestic level, the United States should better define and expand its lexicon regarding force in the cyber domain. Doing so will give legal meaning to the threshold that triggers the inherent right to respond in self-defense. Internationally, barring the ratification of a multilateral treaty, the United States should accept the jurisdiction of the ICJ, which in turn should issue an advisory opinion or a decision in a contentious case outlining specific norms pertaining to the cyber context. Finally, Part V reiterates that if the DoD Manual Cyber Operations chapter represents U.S. policy governing self-defense,[18] it violates U.S. obligations under Charter-based and customary international law.

---

[16] *See* discussion *infra* Part III.A.3 (analyzing the bifurcated role of proportionality).
[17] *See id.*
[18] *Harvey Rishikof, Senior Couns., Crowell & Morning, LLP, Remarks at the Center for Strategic and International Studies: The Role of the U.S. Military in Cyberspace* (Oct. 9, 2015), http://csis.org/event/role-us-military-cyberspace (asserting that cyber-force thresholds are fundamentally legal questions that will be answered by States' policies).

II. BACKGROUND

The international norms governing when States may legally resort to force are based upon the body of law known as *jus ad bellum*,[19] meaning the legal obligations leading up to the outbreak of hostilities.[20] The international community generally accepts the proposition that the normative, Charter-based framework applies to uses of cyber-force or cyber-attacks[21] to the extent that physical effects are analogous to their respective kinetic equivalent.[22] The United States concurs in this analogous, effects-based application of the normative framework to cyber operations.[23] Thus, as an initial matter, it is necessary to briefly outline that legal architecture before moving to an assessment of the specific complexities inherent in the cyber context.

---

[19] "The law of armed conflict, also known as international humanitarian law, is formed by two bodies of law: *jus ad bellum* and *in bello*." *E.g.*, Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE 283, 284 (2012), http://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf. The former pertains to when force may be used, while the latter regulates how "armed actors may employ force." *Id.*

[20] *Jus belli* is the "law of nations as applied to a state of war" and defines the particular rights and obligations of States party to a conflict. *Jus belli*, BLACK'S LAW DICTIONARY 858 (6th ed. 1990). The preposition *ad* means "until" and describes the law up to the initiation of hostilities. *Id.* at 36. Conversely, *in* "express[es a] relation of presence, existence . . . [and] action." *Id.* at 758.

[21] Clearly delineating the meaning of rhetorical choices is necessary towards a proper understanding of legal implications and consequences. *See* Laurie R. Blank, *Cyberwar Versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICT 76, 78 (Jens David Ohlin et al. eds., 2015) [hereinafter *Cyberwar Versus Cyber Attack*]. As used herein, the term "cyber-force" refers to the normative "use of force" within the cyber context; "cyber-attack" carries the meaning of "armed attack"; and "kinetic" refers to the physical context.

[22] Cyber operations, which directly result in physical harm, equate to uses of force. *Cf.* Schmitt, *supra* note 12, at 573 ("[I]t would be . . . absurd to suggest that cyber operations that generate consequences analogous to those caused by kinetic force lie beyond the prohibition's reach . . . .").

[23] *See generally* Harold H. Koh, Legal Adviser, Dep't of State, *Address to the USCYBERCOM Inter-Agency Legal Conference, "International Law in Cyberspace"* (Sept. 18, 2012), *in* SPEAKING THE LAW: THE OBAMA ADMINISTRATION'S ADDRESSES ON NATIONAL SECURITY LAW 370, 372-73 (2015) (suggesting that, if the effects of a use of cyber-force or cyber-attack are analogous to their kinetic equivalent, then responsive rights are likewise analogous).

Subpart A lays the groundwork, discussing the normative framework governing cyber operations, while Subpart B applies that framework to new technologies. Subpart C introduces the bifurcated nature of proportionality as a binding norm of customary international law. Next, Subpart D compares the differences in interpretation between the United States and international community regarding the application of customary law to the cyber context. Finally, Subpart E introduces two examples, the Stuxnet virus and the Office of Personnel Management hack (OPM hack), which will highlight the issues inherent in the current DoD Manual policy.

A. The Jus ad Bellum Framework Governing Cyber Operations

The post-World War II international legal order is founded upon the supremacy of the U.N. as the arbiter of international peace and security.[24] Specifically, the Charter confers upon the Security Council the primary responsibility of maintaining international peace and security.[25] Moreover, the Charter compels Member States to subordinate and limit their impermissibly forceful or aggressive actions to those sanctioned by the Security Council.[26]

---

[24] Following World War II, the Allied powers sought to complicate the exercise of any single State's war prerogative and instead aimed to promote collective security through diplomacy, valuing preservation of the status quo. *See* ANTHONY CLARK AREND & ROBERT J. BECK, INTERNATIONAL LAW AND THE USE OF FORCE: BEYOND THE UN CHARTER PARADIGM 34 (1993) ("[T]he delegates of the San Francisco Conference were convinced that force was simply too destructive to be considered an acceptable means of pursuing changes or advancing other policy . . . . [F]orce was to be used only for value conservation [rather than] value extension.") (footnotes omitted) (internal quotation marks omitted); *see also* U.N. Charter pmbl. ("The Peoples of the United Nations [are] determined . . . to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest . . . .").

[25] Article 7 establishes the principle organs of the U.N., including the Security Council. U.N. Charter art. 7. Chapter V enumerates the responsibilities and competences of the Council. *See id.* arts. 23-32.

[26] *Id.* art. 24, para. 1 ("Members . . . agree that . . . the Security Council acts on their behalf."); *id.* art. 25 ("Members . . . agree to accept and carry out the decisions of the Security Council . . . .").

International law, both Charter-based and customary,[27] expressly prohibits the use of force in a State's conduct of international relations.[28] States are exempt from this prohibition only in instances where forceful action is authorized by the Security Council[29] or as an exercise of a State's inherent right to respond in self-defense to an armed attack.[30] This normative framework is accepted by States as customary international law, so it is binding regardless of individual States' membership in the U.N.[31]

The Charter implies that threshold distinctions separate impermissible uses of force from armed attacks against another

---

[27] While Charter-based and customary international law interact with and inform each other, the legal authority of the two are separate. *See* 48 C.J.S. *International Law* § 2. The Charter gains its authority primarily as a treaty agreed to by all members. *Id.* Thus, the Charter is directly binding only on States party to that agreement. Customary international law is based upon State practice, as well as an understanding that such practice is conducted out of a sense of legal obligation. *Id.* International law is binding on all States regardless of an explicit acceptance to be bound. *Id.* Thus, the Charter is "not only an institution-creating document; it was also a norm-creating document." There are some portions of the Charter that are considered customary international law. AREND & BECK, *supra* note 24, at 29-30.

[28] The customary norm is codified in the Charter under Article 2(4). U.N. Charter art. 2, para. 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.") *see, e.g.*, Schmitt, *supra* note 12, at 572 (discussing the nature of Article 2(4) as a customary norm).

[29] Chapter VII of the Charter, particularly Articles 39 and 42, establishes a legal exception to the Article 2(4) prohibition on the use of force if sanctioned by the Security Council. *Compare id.* art. 2, para. 4 (prohibiting the use of force), *with id.* art. 24, para. (conferring "primary responsibility for the maintenance of international peace and security" on the Security Council) *and id.* art 39 ("The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall . . . decide what measures shall be taken . . . .") *and id.* art. 42 ("The Security Council . . . may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security.").

[30] *Id.* art. 51 ("Nothing in the . . . Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.").

[31] Charter-based and customary norms reinforce each other and together are "generally regarded as [binding] rules of international law." AREND & BECK, *supra* note 24, at 29.

State.[32] That distinction, therefore, informs what a victim-State may do in response to escalated uses of force.[33] However, nowhere does the Charter define exactly what acts are prohibited by Article 2(4).[34] Therefore, States must look to persuasive authorities clarifying that prohibition.[35]

In its *Nicaragua* decision, the ICJ sought to clarify and give legal meaning to the thresholds implied within the Charter.[36] In this case, Nicaragua claimed that the United States breached its international obligations by "recruiting, training, arming, equipping, financing, supplying and otherwise encouraging, supporting, aiding, and directing military and paramilitary actions in and against Nicaragua."[37] From this breadth of alleged activities, the ICJ attempted to delineate a spectrum of impermissible force.[38]

---

[32] *Compare* U.N. Charter art. 2, para. 4, *with* U.N. Charter art. 51 (contrasting the general prohibition on the use of force with the "inherent right" to respond self-defensively "if an armed attack occurs").

[33] A lawful use of force by one State against another is limited by the circumstances contemplated within the Charter's exceptions to Article 2(4). *See supra* text accompanying notes 29-30.

[34] *See* Lieutenant Andrew Moore, *Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models*, 64 NAVAL L. REV. 1, 8 (2015) (noting the lack of definitional precision regarding the prohibition on force within Article 2(4)). While Article 2(4) does not specifically define "use of force," other articles help flesh out the broader definitional boundaries: Article 41 enumerates a non-exhaustive list of potential actions which do not qualify as a use of force, while Article 42 lists specific actions that definitively do constitute uses of force. U.N. Charter arts. 2, 41-42.

[35] *E.g.*, MOHAMED SAMEH M. AMR, THE ROLE OF THE INTERNATIONAL COURT OF JUSTICE AS THE PRINCIPAL JUDICIAL ORGAN OF THE UNITED NATIONS 127-29 (2003) (clarifying that the applicability of Charter-based rules to new situations is possible, in great part, through interpretation by the ICJ).

[36] *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

[37] *Id*. para. 15. Regarding what became known as the "Iran-Contra Affair" the Republic of Nicaragua brought a claim against the United States alleging, *inter alia*, violations of Charter Article 2(4) and the customary prohibition on using force. *See generally* Richard L. O'Meara, *Applying the Critical Jurisprudence of International Law to the* Case Concerning Military and Paramilitary Activities in and Against Nicaragua, 71 VA. L. REV. 1183 (1985) (discussing the background, litigation history, summary of the proceedings, and reasoning behind the judgment).

[38] *E.g.*, Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CAL. L. REV.

Despite the United States' rejection of the ICJ's jurisdiction to decide international legal issues,[39] the Court nonetheless reached a decision regarding illegal uses of force—particularly in identifying an effects-based analysis.[40] By assessing the outcomes—the scope and magnitude—of certain uses of force, the ICJ defined the force spectrum with a low-level boundary, "coercion."[41] Above that, *Nicaragua* emphasized the differential between impermissible force and an armed attack based on severity.[42] Therefore, at the extreme, an armed attack is the most severe use of force, permitting an immediate self-defensive response by the victim-State pursuant to Article 51 of U.N. Charter.[43]

However, even outside the more ambiguous context of the cyber domain, the exact boundaries of impermissible force are determined by an outcomes-based, case-specific analysis and are

1079, 1115 (2013) (clarifying the ICJ's ruling in Nicaragua on the distinctions justifying use of force threshold drawn by the ICJ in).

[39] *Nicar.*, 1986 I.C.J. para. 10.

[40] *Nicaragua* stands for the proposition that the gravity of a use of force, or the effects incurred by the victim-State, define the threshold above which said victim-State may seek to respond. *See id.* para. 14. Thus, the legally available response to force is necessarily limited by the severity of force precipitating the response. *Id.*

[41] In *Nicaragua*, the ICJ recognized threshold distinctions separating uses of force from coercive acts, the latter being governed by the principle of State sovereignty and not force. *Id.* para. 205. A State may promulgate internal policies that impact others, in effect, so long as it does not directly intervene in the internal processes of another. *Id.* ("A prohibited intervention [bears] on matters in which each State is permitted, by the principle of State sovereignty, to decide freely.") (meaning domestic economic or political policies that influence—but do not intervene in—other States are not illegal).

[42] In its decision, the ICJ evaluated the alleged material support provided by the United States to the Contras, including funding, logistical and military support, and the planning and execution of military objectives on Nicaraguan facilities. *Id.* paras. 81–86, 228. The Court found that direct military assistance constituted an impermissible use of force, but not an armed attack. *Id.* para 195.

[43] "An armed attack is more severe significant than a use of force, meaning that a state can be the victim of a use of force without being the victim of an armed attack that triggers the right of self-defense." *Cyberwar Versus Cyber Attack*, *supra* note 21, at 90. The predicate to any lawful self-defensive force is the existence of an armed attack in the first instance. *Id.*

unclear at times.[44] Conversely, the "attack" threshold is delineated by a grave act of targeted violence.[45] It is determined by the severity of force used, measured by the effects, as well as the intent behind the perpetration of the act itself.[46] Dovetailing with the use-of-force effects analysis, in 1974, the General Assembly of the United Nations (General Assembly) passed a resolution outlining a non-exhaustive list of acts that constitute "attack[s] by armed forces."[47] In the so-called Definition of Aggression,[48] each example is designated pursuant to the action taken—the aggressive, military purpose—as well as the resultant effect.[49]

The takeaway from this normative framework, as it pertains to the threshold above impermissible uses of force, is that customary international law—informed by the Charter-based legal architecture—is organized by gradations.[50] The divisions

---

[44] *See* Moore, *supra* note 34, at 12 (noting that the physically damaging effects, and not the type of tool employed, renders a use of force counter to the purposes of the U.N. Charter).

[45] In the *jus ad bellum*, "attack" has a particular meaning—the most grievous use of force—as employed in Article 51 of the Charter, and clarified by *Nicaragua*. *See cf.* Schmitt, *supra* note 19, at 285-87 (distinguishing "armed attack" as a term de art and noting the "gap" separating a use of force from an "attack", where the latter is sufficient to trigger a self-defensive response). This is distinct from the *jus in bello* meaning of "attack." *Id*. at 285 (clarifying that international humanitarian law aims to restrict "attacks" within active hostilities so as to minimize harm). Once an armed conflict is underway, "attacks" are defined as "acts of violence against the adversary, whether in offence or defence," and are lawful so long as they proportionally target legitimate military objectives. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) arts. 48, 49(1), June 8, 1977, 1125 U.N.T.S. 3.

[46] *Cf.* Schmitt, *supra* note 19, at 287 (noting that "Article 51 adopts an 'act-based' threshold using a specified type of action rather than one based on particular consequences.").

[47] These include, but are expressly not limited to, attacks within the traditional domains of armed forces by one State on another. Definition of Aggression, arts. 3-4, U.N. GAOR, 29th Sess., 2319th plen. mtg. at 143, U.N. Doc. A/8082.

[48] *See generally id*. (providing a definition of aggression by resolution of the General Assembly to "contribute to the strengthening of international peace and security").

[49] *See id.* at art. 3.

[50] *Cf.* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14, para. 228 (June 27) (noting a relative distinction in the nature of certain acts within the meaning of the customary prohibition on the use of force).

established by the corresponding thresholds form the basis for a legal response by a victim-State,[51] and these thresholds are defined by a scope-and-magnitude effects analysis.[52] Crucially, a State must have been a victim of an armed attack in order to legally access its inherent right to respond in self-defense.[53]

B. Framework 2.0: New Technologies and Prohibited Force

The normative framework is not so restrictive as to prevent evolution within the law or to ignore changing realities; rather, it was designed with an eye toward elasticity and adaptability.[54] Indeed, the ICJ has noted that where generic terms are used in longstanding or perpetual treaties, "the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning."[55] Certainly, the Charter qualifies as such a treaty, and the prohibition on use of force—as customary law—represents a concept that falls within these terms.[56]

---

[51] *Id.*

[52] *Id.* para. 195.

[53] Self-defense is governed by the formulation that arose out of the diplomatic snafu surrounding the "Caroline Incident." *E.g.*, Laurie R. Blank, *A New Twist on an Old Story: Lawfare and the Mixing of Proportionalities* [Hereinafter *A New Twist*], 43 CASE W. RES. J. INT'L L. 707, 714 (2011). In the mid-nineteenth century, during a Canadian uprising against the Crown, British troops crossed the Niagara River and torched the Caroline, a U.S. steamship, that was allegedly transporting arms to the Canadian rebels. *See* AREND & BECK, *supra* note 24, at 18. The British claimed self-defence. *A New Twist*, *supra* note 53, at 714. Daniel Webster, then-Secretary of State, wrote to Lord Ashburton, his British counterpart, declaring that self-defensive force should be circumscribed to "cases in which the necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation." Hunter Miller, *British-American Diplomacy The Caroline Case*, AVALON PROJECT http://avalon.law.yale.edu/19th_century/br-1842d.asp (last visited Jan. 26, 2017) (reproducing a letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, Special British Minister).

[54] For instance, the Definition of Aggression identified the then-dominant domains of warfare, but noted that its list was not exhaustive. *See* Definition of Aggression, *supra* note 47 (intending for this guidance to have staying power, it ensured as much by noting that the Security Council could amend the list at any time).

[55] MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 20-21 (2014) (quoting another source).

[56] *See supra* text accompanying note 27 (clarifying the customary nature of Article 2(4)).

Additionally, the ICJ provided explicit legal analysis supporting the general applicability of this framework to new technologies in its *Nuclear Weapons Advisory Opinion (Nuclear Weapons)*.[57] In *Nuclear Weapons*, the Court specifically addressed the issue of weapons governed by the prohibition on force, which Article 2(4) neglected at the time of its drafting.[58] *Nuclear Weapons* holds that the prohibition on force is ambiguous to the deployment of any single type of weapon but is governed by the effects-based analysis laid out in *Nicaragua*.[59] Moreover, the international community broadly supports the applicability of this normative framework to new developments and capabilities, including in the cyber context.[60] Indeed, the United States has been explicit in its agreement that where the effects of a use of cyber-force or cyber-attack are analogous to a kinetic use of force or armed attack, the rights of responsive action are likewise analogous.[61]

C. Proportionality as a Rule of International Law

The legal scheme instituted by the Charter enforces the Article 2(4) prohibition, in part, by obstructing the potential escalation of responsive action, thus serving the institutional purpose of the U.N.[62] The Charter framework is buttressed in this

---

[57] *See generally* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226 (July 8).
[58] *Id.*
[59] *Id.* paras. 39-40.
[60] *See* ROSCINI, *supra* note 55, at 20-30 (discussing the broad international consensus on the applicability of kinetic treaties and customs to the cyber context).
[61] *See, e.g.*, Koh, *supra* note 23, at 372-73. Of course, the problem here, and the central conflict addressed by this Comment, is that the United States recognizes the framework, but not the applicability of the thresholds required by *Nicaragua*. Especially in the cyber context, where these thresholds are so ill-defined, the right claimed by the United States to respond in self-defense is particularly in conflict with the Charter-based and customary norms outlined by the framework above. *See* discussion *infra* Part III (analyzing the contradictions of U.S. cyber policy and its international legal obligations).
[62] Schmitt, *supra* note 19, at 286 ("[T]he central object and purpose of the United Nations [is] to craft a system that effectuates a strong presumption against the use of force in international relations . . . .").

effort by certain international legal norms.[63] Of particular note is the principle of proportionality, which has its origins in Just War theory and stands for "the fundamental principle that belligerents do not enjoy an unlimited choice of means to inflict damage on the enemy."[64]

Proportionality is a *jus ad bellum* and *in bello* rule of international law.[65] In *Nicaragua*, and elsewhere, the ICJ has reaffirmed that proportionality relates to the "degree of force needed to eliminate the danger or repel the attack."[66] Thus, a violation occurs only when the victim responds with more force than reasonably required to deter or defeat the threat,[67] which is true of both proportionalities *ad bellum* and *in bello*.[68] Regarding the latter, the use of force in response to a substantially low-level use of force constitutes a forceful reprisal.[69]

---

[63] Legal self-defensive force relies, *inter alia*, on necessity and proportionality. *See, e.g.*, David Kretzmer, *The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum*, 24 EUR. J. INT'L L. 235, 239 (2013). Regarding the former, "necessity" restricts the resort to force to those necessary to achieve the legitimate end of suppressing the initial attack—it need not be the only option, but it must be reasonably calculated to curb the immediate threat. *Id.*; *see also supra* note 53 and accompanying text.

[64] Judith Gail Gardam, *Proportionality and Force in International Law*, 87 AM. J. INT'L L. 391, 391 (1993). Under Just War theory, proportionality imposed an assessment that balanced the evil of war with the overall good achieved by conflict. *Id.* at 394-95. Unlike the modern, secular proportionality requirement, the emphasis in Just War theory was on the justness of the cause itself. *Id.*

[65] The legal weight of proportionality, as a norm prior to (*ad bellum*), as well as within conflict (*in bello*), has two specific applications: the former, regarding "the relationship between an act and the legitimate response to that act"; and the latter, relating to a means-ends analysis, where the harm must not outweigh the expected benefit. Kretzmer, *supra* note 63, at 238.

[66] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 para. 237 (June 27); *see also* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, para. 41 (July 8); Oil Platforms (Islamic Republic of Iran v. U.S.), 2003 I.C.J. Rep. 161, paras. 43, 76 (Nov. 6) (separate opinion of Judge Simma).

[67] *See A New Twist*, *supra* note 53, at 43 (noting that the primary purpose of self-defense is to halt and repel an attack).

[68] *See* Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 AM. J. INT'L L. 715, 720 (2008) (emphasizing that proportionality constrains lawful forcible responses even within the legitimate exercise of self-defense).

[69] C*f.* AREND & BECK, *supra* note 24, at 42 (clarifying that "reprisals" are necessarily punitive: "they seek to impose reparation for the harm done") Since

D. The Tallinn Manual: Customary Rules for Cyber Operation

In 2013, an International Group of Experts[70] sought to clarify and codify customary law in the cyber operational domain.[71] The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual) enumerates ninety-five *black-letter* rules,[72] representing the *lex lata* customary norms in the cyber context.[73] While the specific contours of States'

---

a reprisal, by definition, is responsive to a perceived injury below an armed attack—and possibly also below a use of force—it necessarily represents an illegal use of force governed by the customary and Charter-based prohibition thereon. *Id.*

[70] The Group of Experts was composed of academics and practitioners from the Australia, Belgium, Canada, Germany, the Netherlands, Sweden, Switzerland, the United Kingdom, the United States, and technical experts from the NATO Cooperative Cyber Defence Center of Excellence; working by consensus to evaluate the existence of customary international norms. INT'L GROUP OF EXPERTS AT THE INVITATION OF THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE x–xiii (2013), https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [hereinafter TALLINN MANUAL]. They were assisted in this endeavor by official observers from NATO Allied Command Transformation, U.S. Cyber Command, and the International Commission of the Red Cross. *Id.* at 6. The official observers from NATO Allied Command Transformation, U.S. Cyber Command, and the International Commission of the Red Cross participated fully in the discussion, but were not included in the unanimity required to codify the rules. *Id.*

[71] *E.g.*, *id.* at 3 (discussing the range of international approaches to the application of the normative framework to cyber and the need to clarify States' obligations).

[72] *Id.* at 11. Defining "rules" is somewhat of a misnomer; the customs codified in the Tallinn Manual represent norms, as interpreted by the Group of Experts. *Id.* at 1. "It is essential to understand that the Tallinn Manual is not an official document, but . . . . must be understood as an expression solely of the opinions of the International Group of Experts . . . ." *Id.* at 1 (noting that, though it is influential as an interpretation of State practice and *opinio juris* regarding cyber operations, the Tallinn Manual represents a consensus-driven process of non-binding assessments as to the current state of customary international law); *id.* at 6 ("To the extent that the Rules accurately articulate customary international law, they are binding on all States . . . .").

[73] *Id.* at 5 (discussing that *lex lata* is the law as it stands—in this case, as of 2013. The Tallinn Manual expressly does not attempt to examine the *lex ferenda*).

obligations are unclear or potentially in flux,[74] the Group of Experts was unanimous in its assertion that the normative framework, as to permissible responsive action following an armed attack, applies to the cyber context.[75]

The Tallinn Manual and DoD Manual offer the best comparison between the legal interpretation of the international community and that of the United States[76] regarding States' obligations in the cyber domain.[77] Both broadly concur that the Charter-based prohibition applies to the cyber context,[78] and a State may access its inherent right to self-defense when attacked.[79] This is particularly clear where the effects of a use of cyber-force or a cyber-attack are analogous or equate to the resultant harm

---

[74] *Id.* at 6 (noting that the commentary accompanying each rule underscores disagreement among the experts as to the contours of the norm, identifies the legal basis and normative content for the rule, and addresses practical implications).

[75] *Id.* at 5. As representatives of the international community, the experts recognized that ambiguities within the cyber context bred confusion as to the contours of States' international legal obligations, but not that such obligations governed conduct within the cyber context. *Id.* at 3. "The International Group of Experts was unanimous in its estimation that both the *jus ad bellum* and *jus in bello* apply to cyber operations." *Id*. at 5. "Its task was to determine how such law applied, and to identify any cyber-unique aspects thereof." *Id.* at 3.

[76] The Tallinn Manual is a persuasive, but limited legal interpretation of customary law, much like the policy perspective codified in the DoD Manual. *Compare id.* at 1, 6 (noting that no obligations emanate directly from the Tallinn Manual, but to the extent that it reflects customary law, all States are bound by the rules therein), *with* LAW OF WAR MANUAL, *supra* note 1, at iii (limiting the scope of the DoD Manual to a Department-wide resource for DoD personnel).

[77] Military manuals are not, themselves, authoritative regarding overarching international customary principles, but may be referenced as evidence of States' acceptance thereof. *Cf.* TALLINN MANUAL, *supra* note 70, at 9 ("[M]ilitary manuals are . . . cited . . . for the purpose of alerting the reader to a State's acceptance of the general legal principle involved.").

[78] *Compare* TALLINN MANUAL, *supra* note 70, at 5 (noting unanimity amongst the International Group of Experts), *with* LAW OF WAR MANUAL, *supra* note 1, at 987 (asserting the applicability of certain law of war rules to cyber operations "even though these rules were developed long before cyber operations were possible.").

[79] *Compare* TALLINN MANUAL, *supra* note 70, at 54 ("Rule 13 - . . . A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence."), *with* LAW OF WAR MANUAL, *supra* note 1, at 990-91 (confirming that a State's inherent right to self-defense pursuant to Charter Article 51 translates to the cyber domain).

caused by a kinetic use of force or attack.[80] Therefore, cyber attacks that "trigger a nuclear plant meltdown . . . [or] open a dam above a populated area, causing destruction" would constitute an armed attack.[81]

However, the concurrence between the Manuals ends there. The international community, through the Tallinn Manual, reiterates the *Nicaragua* scale-and-effects test.[82] Conversely, the DoD Manual claims that cyber operations constituting "any illegal use of force" may "give[] rise to a right to take necessary and proportionate" self-defensive action.[83] Thus, the two Manuals represent a distinct conflict of interpretation regarding operations within the cyber domain.

E. Cyber Operations & Uses of Force

To illustrate the unique problems posed by the Cyber Operations chapter in the DoD Manual, this Comment summarizes two recent cyber operations: the Stuxnet virus, deployed against Iran, and the OPM hack.[84]

1. Stuxnet Virus (2010)

---

[80] *Compare* TALLINN MANUAL, *supra* note 70, at 48 ("[Cyber] [a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force . . . ."), *with* LAW OF WAR MANUAL, *supra* note 1, at 988 (asserting an effects-based analogy giving rise to responsive action).

[81] LAW OF WAR MANUAL, *supra* note 1, at 989 (discussing actions that cause direct and damaging physical results, such as crashing an airplane). Particularly where infrastructure damage has been sustained and deaths occur, the United States makes a clear analogous determination that a cyber-attack constitutes a use of force triggering self-defense within the meaning of Article 51. *Id.*; *see also* TALLINN MANUAL, *supra* note 70, at 55 ("[A]ny use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement [for an armed attack].").

[82] *See* TALLINN MANUAL, *supra* note 70, at 45.

[83] *See* LAW OF WAR MANUAL, *supra* note 1, at 991 (noting that the United States asserts this right pursuant to paragraph 16.3.3.1).

[84] As international law is fundamentally a State-to-State construct, for a victim-State to respond, the initial use of force must be attributable to a State actor (either directly or with a duty of care to suppress acts within its territory). *See, e.g.*, Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELB. J. INT'L L. 496, 506 (2013). Thus, for the purposes of the Stuxnet virus and OPM hack examples, this Comment assumes State attributability. *See infra* notes 90, 94 and accompanying text.

On a visit to Iran in 2010, inspectors from the International Atomic Energy Agency noticed that centrifuges at the Natanz enrichment center were failing at an abnormally high rate, despite reparative efforts by Iranian technicians.[85] Eventually, researchers located a malware virus within the Iranian system called Stuxnet.[86] The virus operated between June 2009 and May 2010, with two predominant purposes.[87]

> First, it includes code that, when executed, dramatically raised and lowered the centrifuges' rotational speed, causing the centrifuges to destroy themselves. Second, the worm sent signals to plant operators indicating that the centrifuges were working normally, so that the operators were not alerted to the problem and were unable to prevent the centrifuges from self-destructing.[88]

Based on analysis of the code, the United States and Israel were most likely responsible for the malware.[89]

2. Stuxnet Virus (2010)

---

[85] *See* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON 1, 3 (2014) (commenting generally on the weaponization of the cyber domain, as well as the specific circumstances surrounding the Stuxnet virus).

[86] Bruce Schneier, *The Story Behind the Stuxnet Virus*, FORBES (Oct. 7, 2010, 6:00 AM), https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#d1bd7a051e83.

[87] *See* ROSCINI, *supra* note 55, at 6.

[88] Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate A Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 844 (2012) (explaining how Stuxnet went unnoticed while damaging Iran's centrifuges). The Stuxnet Virus carried a so-called "weaponized" payload, the first known malicious code deployed to cause physical damage to a national critical infrastructure. *See* ROSCINI, *supra* note 55, at 6.

[89] Richmond, *supra* note 88, at 843. Upon analysis of the code found at Natanz, it is at least plausible that the United States and Israel developed the Stuxnet Virus, covertly deploying it as an alternative to kinetic force in an effort to derail Iran's nuclear ambitions. *See id.* at 843-44. Naturally, neither State has claimed responsibility. *Id.* at 845. For clarity, this Comment will assume attributability for Stuxnet to the United States and Israel.

In June 2015, OPM[90] announced that it had been hacked and that the personal information of U.S. government employees and individuals listed on employees' background checks had been compromised.[91] Roughly two weeks later, OPM identified another hack, this time targeting security clearance forms.[92] The intent of the perpetrators and the full extent of damage caused by the breach are not publically known; however, the United States attributes the OPM hacks to the Chinese government.[93]

III. ANALYSIS

The 2016 DoD Manual reaffirms that cyber is an important operational domain but also that the United States' interpretation of its international legal obligations is a comparatively blunt instrument. The lack of nuance regarding threshold distinctions between a use of force and an armed attack in the cyber context is legally problematic given the definitional ambiguities within that domain.[94] By claiming a right to potentially respond to "any illegal

---

[90] OPM is responsible for human resources within the U.S. Federal Government. OFFICE OF PERSONNEL MGMT., *Our Mission, Role & History: What We Do*, OPM.GOV, https://www.opm.gov/about-us/our-mission-role-history/what-we-do/ (last visited Jan. 26, 2017) [hereinafter *Our Mission*] ("We're responsible for keeping the government running smoothly—a responsibility that has daily consequences for every citizen.").

[91] OFFICE OF PERSONNEL MGMT., *Cybersecurity Resource Center: Cybersecurity Incidents*, OPM.GOV, https://www.opm.gov/cybersecurity/cybersecurity-incidents (last visited Jan. 26, 2017) [hereinafter *Cybersecurity*] (concluding with "high confidence that sensitive" employee background information, including social security numbers and fingerprints, had been accessed).

[92] Kristen Eichensehr, *The OPM Hack and the New DOD Law of War Manual*, JUST SECURITY (June 17, 2015, 9:37 AM) [hereinafter *The OPM Hack*], https://www.justsecurity.org/23960/opm-hack-dod-law-war-manual.

[93] Ellen Nakashima, *Chinese government has arrested hackers it says breached OPM database*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html (reporting that U.S. officials suspect the Chinese Ministry of State Security was responsible). For clarity, this Comment will assume attributability for the OPM hack to China.

[94] The DoD Manual acknowledges the unsettled legal nature of the cyber context and implicitly recognizes the need for identifiable principles and rules of law to govern operations in that domain. LAW OF WAR MANUAL, *supra* note 1, at 987 (making it clear that, where settled rules are absent, defined legal principles

use of force," the U.S. policy is in conflict with international law: both the Charter-based prohibition on force and the customary principles of *jus ad bellum* and *in bello* proportionality.[95]

A. U.S. Cyber Policy Violates the Prohibition on Force

If the United States were to act upon its policy of non-distinction regarding use of force and armed attack, it would violate international law.[96] In reserving the right to take per se responsive action, the United States rejects the normative framework as it pertains to legal force.[97] The DoD Manual articulates a policy that contravenes binding obligations enshrined in the Charter, as well as the prohibition on force in customary law, as codified in the Tallinn Manual.[98] This is particularly clear in the context of the OPM hack, if the United States were to improperly invoke a right to self-defensive response against China.[99]

1. The U.N. Holds Sovereign Authority Over Lawful Force

---

must control States' conduct to ensure proper access to their rights and obligations under international law).

[95] *E.g.*, James E. McGhee, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy*, 2 J. L. & CYBER WARFARE 64, 94-101 (2013) (discussing the relative novelty of cyber operations and potential legal consequences of U.S. policy therein).

[96] *See* James E. McGhee, *Hack, Attack or Whack; the Politics of Imprecision in Cyber Law*, 4 J. L. & CYBER WARFARE 13, 24-26 (2014) [hereinafter *Hack, Attack or Whack*] (cautioning against imprecision regarding rights and obligations within the cyber context).

[97] *See supra* text accompanying note 29; *see also infra* text accompanying note 105 (highlighting the legal architecture created by the Charter, and the exclusive power of the Security Council to check a State's ability to escalate responsive action).

[98] *Compare* TALLINN MANUAL, *supra* note 70, at 45, *with* LAW OF WAR MANUAL, *supra* note 1, at 991 (noting the contradiction between the two manuals, particularly in the U.S. rejection of thresholds clarified by *Nicaragua*).

[99] The DoD Manual's Cyber Operations chapter is heavily dependent on analogy to physical effects. *See, e.g.*, LAW OF WAR MANUAL, *supra* note 1, at 994-95 (referencing cyber operations that attack infrastructure, for instance, causing damage to nuclear reactors, airplanes, and dams). Since the OPM hack has neither resulted in physical damage, or directly caused death, it is far from clear that it constitutes even a use of cyber-force within the meaning of Article 2(4). *Cf*. *Cybersecurity*, *supra* note 91.

By rejecting threshold distinctions in the cyber operational domain, the DoD Manual runs counter to U.S. obligations under the Charter. In 1948, the U.N. instituted a new "normative" legal order, which codified the prohibition on the use of force in international relations and created a scheme for enforcement.[100] Neither Article 2(4) nor the customary norm prohibiting force is "remedial in nature"; rather, both establish "threshold[s] for breach of international law."[101] As such, a State's response must be determined either by the Security Council's scope of authority or via a State's inherent right to self-defense.[102] Here, the United States implicitly rejects the purpose of the Charter to impose an external check on a State's ability to resort to force.[103]

To comply with the prohibition, a victim-State's ability to legitimately respond with force is limited by the gravity of the initial force uncured in all instances short of an armed attack.[104] In effect, the Charter-based legal architecture fulfills the purpose of the United Nations[105] by vesting the Security Council with a limited, but exclusive, sovereignty over the international exercise of lawful force.[106] The Charter implies, and *Nicaragua* clarifies,

---

[100] *Cyber Revisited*, *supra* note 12, at 570.
[101] *Id.* at 572-73.
[102] *Id.*
[103] The role of the ICJ is to interpret the general rules set out in the Charter; it is competent to perform this function as the designated judicial arm of the U.N. *See* AMR, *supra* note 35, at 127-29 (emphasizing the role of the ICJ as an interpreter of the Charter). By rejecting *Nicaragua*, the United States ignores this crucial purpose, and in so doing rejects the nuance required by the Charter in effectuating its prohibition on the use of force. *Cf.* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14 (June 27) (delineating gradations of uses of force and the necessarily threshold for responsive self-defense).
[104] *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14 (June 27)..
[105] On a textual analysis, the primary purpose of the U.N. is "to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression." U.N. Charter art. 1, para. 1.
[106] Sovereignty over certain competencies vests in an institution where no other authority above that institution is "endowed with the legal power to constrain" the exercise of that function. Guglielmo Verdirame, *A Normative Theory of Sovereignty Transfers*, 49 STAN. J. INT'L L. 371, 411 (2013) (discussing the transfer of limited sovereignty from States to the Security Council, particularly regarding lawful force). By virtue of membership in the U.N., States cede to the

that the gravity of the initial illegal use of force determines the threshold response available to the victim-State.[107] Should that initial force be less severe in its effects than what constitutes an armed attack, a State does not have, and may not invoke, a right to self-defense.[108] Should it wish to respond, the victim-State must seek approval from the Security Council and, in so doing, reinforce that body's sovereignty over use of force in international disputes.[109]

The Tallinn Manual and the DoD Manual support different theories of sovereignty. The former adheres to the normative framework, ceding authority over legal force to the Security Council, except where a precipitating use of force of sufficient magnitude triggers an Article 51 exception to the prohibition.[110] Conversely, the DoD Manual asserts a sovereign right to respond held by the State that is limited only by internal assessments of necessity and proportionality.[111] This construction violates the legal architecture created by the Charter.[112]

The United States supports the notion that the normative framework governs cyber operations[113] but rejects the primary,

---

Security Council [their] authority to wage legal war, pursuant to Articles 24, 39, and 42 of the Charter. *See supra* text accompanying notes 29, 106.

[107] The legal threshold and methods available to a victim-State in response is measured by the gravity of the predicate force and the resulting effects. *See* Nicar. v. U.S., 1986 I.C.J. at 101, para. 191 ("[I]t [is] necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.").

[108] *See* U.N. Charter art. 51 (predicating self-defensive action by a victim-State on a preceding armed attack).

[109] See id. art. 39 (empowering the Security Council to determine the response to uses of force short of an armed attack); *see also supra* text accompanying note 106.

[110] The international community adheres to the spectrum of force delineated in *Nicaragua*. *See* TALLINN MANUAL, *supra* note 70, at 45.

[111] LAW OF WAR MANUAL, *supra* note 1, at 991.

[112] *See supra* text accompanying notes 29, 106 (discussing the interplay of Articles 24(1), 39, and 42 in defining the normative legal architecture of the Charter).

[113] *See, e.g.*, President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* 9 (2011) ("The Development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete.").

external role of the Security Council vis-à-vis force to sanction such action.[114] In failing to incorporate *Nicaragua's* threshold distinctions within the DoD Manual, the United States ignores the contours of international obligations derived from the Charter.[115] In *Nicaragua*, the ICJ articulated a persuasive interpretation of the customary prohibition on the use of force.[116] The DoD Manual fails to recognize that the most prolific enforcement mechanism for that prohibition—per the U.N. Charter—is the sovereignty vested in the Security Council over the international use of force.[117]

As a matter of treaty law, the United States is bound to uphold the purpose of the U.N., of which it is a member.[118] Thus, the position promulgated by the DoD Manual, that the United States may disregard distinctions within uses of cyber-force, violates that obligation.[119] Pursuant to the sovereignty of the Security Council, the United States may not legally claim or exercise an "inherent" right of self-defense in response to uses of cyber-force that do not rise to the level of an armed attack.[120] Doing so bypasses the U.N.'s enforcement mechanism, pursuant to

---

[114] *Cf.* Koh, *supra* note 23, at 377 ("In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response.").

[115] Conversely, the Tallinn Manual explicitly references State obligations and the precipitating thresholds allowing for lawful self defense, as clarified in *Nicaragua*. *See Tallinn Manual*, *supra* note 70, at 45.

[116] *Cf. supra* text accompanying note 35.

[117] The Charter expressly empowers the Security Council to determine the appropriate and legal redress, including forceful countermeasures. *See supra* text accompanying note 29.

[118] *See, e.g.*, LAW OF WAR MANUAL, *supra* note 1, at 36 n.161 ("Every treaty in force is binding upon the parties to it and must be performed by them in good faith.").

[119] Since *Nicaragua* clarifies distinctions implied by the Charter, a State acting in good faith of its treaty obligations should likewise adhere to the inherent call within the Charter to distinguish thresholds. *Cf.* A. Mark Weisburd, *The International Court of Justice and the Concept of State Practice*, 31 U. PA. J. INT'L LAW 295, 296-97 (2009) (noting the principal function of the ICJ as interpreter of the UN Charter and underscoring its authority in outlining the scope and content of customary rules of international law).

[120] As clarified by *Nicaragua*, a State may only invoke its "inherent right to self-defense" pursuant to a precipitating use of force of sufficient gravity to constitute an armed attack, within the meaning of Article 51 of the Charter. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 228 (June 27); *see also* U.N. Charter art. 51.

Articles 24, 39, and 42, which establishes the primacy of the Security Council to authorize any use of force by a victim-State in response to force not rising to the level of an armed attack.[121] Thus, the DoD Manual impermissibly invokes a right that properly emanates only from the Security Council.[122]

2. The Cyber Domain Exacerbates Definitional Ambiguity

Notwithstanding the flexibility and elasticity of the normative framework, the unique problems of the cyber domain exacerbate the overbroad definitional issues inherent in the U.S. position. From a policy or military perspective, broadly defining a State's right to respond to an "illegal" use of cyber force strategically allows for the greatest leeway.[123] However, such rhetorical overgeneralization has serious legal repercussions.[124] Due to the unsettled nature of the norms in this domain, any overbroad language used by States to define their rights can needlessly push cyber activity into the realm of force, as controlled by Article 2(4).[125]

The DoD Manual's over-broad claim to self-defense risks force escalation[126] contrary to the purpose of the U.N. Charter and the customary prohibition on force codified therein.[127] Each rule within the Tallinn Manual is accompanied by commentaries discussing, *inter alia*, alternate interpretations of customary law.[128] This indicates that certain fundamental aspects of the normative

---

[121] *See supra* text accompanying notes 29, 106 (discussing the sovereignty of the Security Council).
[122] *See supra* text accompanying notes 29, 106 (discussing the sovereignty of the Security Council).
[123] *Hack, Attack or Whack*, *supra* note 96, at 38.
[124] *Id.* at 15 (characterizing an event in certain terms, where military force is implicated, "makes all the difference" in authorizing a forcible response).
[125] Kenneth Watkin, *The Cyber Road Ahead: Merging Lanes and Legal Challenges*, 89 INT'L L. STUD. 472, 503 (2013) (arguing that the terminology as applied to cyber pushes such activity into the realm of force).
[126] *Cf.* Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 270 (2009).
[127] *See supra* text accompanying note 24.
[128] TALLINN MANUAL, *supra* note 70, at 6.

framework remain somewhat unstable vis-à-vis cyber.[129] Particularly in this state of legal fluctuation, the permissive U.S. definition of precipitating force in the DoD Manual supports, rather than diminishes, the risk of rapid escalation.[130]

Moreover, the United States recognizes the perils of such over-generalization in the cyber context, yet persists in claiming an extended right to self-defensive action.[131] As a matter of international stability, the United States acknowledges that the unique attributes of cyber require additional clarification.[132] Yet, rather than follow through on its strategy to help solidify cyber norms,[133] the DoD Manual fails to articulate nuance within the definitional spectrum vis-à-vis "illegal use of force" and "armed attack."[134] The United States ignores its own policy interests as well as increases the risk of escalation by asserting a lax definition of its so-called right to respond.[135]

---

[129] *See* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 661-62 (2011) ("[U]ncertainty invites cyber warfare operations during the intermediate [legal] flux . . . ."). The international community's inability to articulate clear norms highlights the dangers of ambiguity, such that escalated activity may go unchecked. *Id.* at 662.

[130] *See* Watkin, *supra* note 125, at 503 (employing warlike terms for expansive cyber activity increases "the potential for misunderstanding and overreaction," with dire consequences).

[131] *See generally International Strategy for Cyberspace*, *supra* note 114 (highlighting U.S. policy goals to help bring structure and stability to the cyber domain through international cooperation and governance).

[132] *Id.* at 9 ("[T]he development of norms for state conduct in cyberspace does not render existing international norms obsolete. . . . Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.").

[133] Highlighting the unsettled nature of legal norms, the United States identified a need to play a formative role. *Id.* The growth of the cyber domain has "not been matched by clearly agreed-upon norms . . . . To bridge that gap, we will work to build a consensus on what constitutes acceptable behavior." *Id.*

[134] *Cf.* LAW OF WAR MANUAL, *supra* note 1, at 991.

[135] *See* Oona A. Hathaway, et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 881 (2012) (arguing that individual States should adopt clear definitions associated with permissible and impermissible actions vis-à-vis the prohibition on force as an intermediary measure leading up to more formal future cooperation).

At this moment in the legal development of the cyber domain, the normative thresholds are ill-defined and too elastic to support such a sweeping definition of acts sufficient to invoke self-defense.[136] As such, the spectrum of cyber activities potentially included in "illegal force" is impermissibly broad.[137] Pursuant to the Tallinn Manual, the distinction between cyber-force and cyber-attack is comparatively clearer,[138] with the international community contemplating greater definitional flexibility regarding that threshold.[139] However, the area below use of cyber force is dangerously muddled.[140]

The utter ambiguity of the lower bound for the use of force poses the greatest threat to the U.S. position. The Tallinn Manual shies away from an analysis of impermissible cyber activity below use of force specifically because the Group of Experts was unable to reach consensus on analogous cyber norms.[141] The combined effect of an unclear lower bound for the use of force, with the broad definition in the DoD Manual, poses a significant risk to the United States, such that it may incorporate excessively low-level

---

[136] *See Hack, Attack or Whack*, *supra* note 96, at 15.

[137] By calculating its response to a cyber- event, which would kinetically constitute non--forceful action, the United States risks creating a spectrum of force rejected by *Nicaragua*. *See supra* text accompanying note 41 (discussing the role of coercion in international law).

[138] *See* Schmitt, *supra* note 19, at 286 (regarding the upper threshold, "the challenge lies in interpreting the adjective 'armed'" in the cyber context within the meaning of Article 51); *see also* Legality of the Threat or use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. ¶¶ 39-40 1996 (July 8) (relying on an effects-based, destructive power, rather than any particular weapon).

[139] Michael Schmitt, an expert on cyber issues and author of the Tallinn Manual, argues that evolving the "Caroline factors" will accommodate the unique complexities of cyber. *Compare Cyber Revisited*, *supra* note 12 (offering a non-exhaustive list of factors, including severity, immediacy, directness, invasiveness, measurability of effects, State involvement, military character, and presumptive legality), *and* TALLINN MANUAL *supra* note 70, at 48-49 (incorporating the Schmitt factors), *with supra* text accompanying note 52 (discussing the Caroline incident and the factors for lawful self-defense defined thereby).

[140] *See e.g.*, TALLINN MANUAL, *supra* note 69, at 3 ("The community of nations is understandably concerned about this normative ambiguity. . . . [T]he unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.").

[141] *See id.* at 4.

cyber-force into its response calculus.[142] Thus, "illegal force" could potentially include an overly broad range of sub-force cyber-events up through proper cyber-attacks.

Far from the brevity currently codified in the DoD Manual, the United States should be exact in its claim to self-defense.[143] The unsettled nature of customary law in the cyber domain exacerbates definitional permissiveness, potentially allowing for a much broader scope of what constitutes "illegal force."[144] Moreover, the overbroad "right" asserted within the Cyber Operations chapter conflicts with the purpose of the U.N. Charter, its prohibition on force, and increases the likelihood that the United States will illegally escalate cyber activity.

3. Collapsing Cyber Thresholds Violates Proportionality

The non-distinction in the DoD Manual regarding use-of-force thresholds not only violates the prohibition on force, but it likewise violates proportionality as a binding customary legal norm.[145] This is true both of the *ad bellum* and *in bello* aspects of the norm.[146] Proportionality is violated by both the invocation of self-defense pursuant to an insufficiently grave cyber event as well as by forceful action in response to a precipitating cyber-force that fails to meet the necessary Article 51 threshold.[147] The DoD Manual acknowledges an internal constraint on forceful responses,

---

[142] *Cf. supra* text accompanying note 129 (showing the ease by which the United States may be over-inclusive regarding its ability to respond to excessively low-level cyber events).
[143] *Cf. supra* text accompanying note 129 (showing the ease by which the United States may be over-inclusive regarding its ability to respond to excessively low-level cyber events).
[144] *Cf. supra* text accompanying note 129 (showing the ease by which the United States may be over-inclusive regarding its ability to respond to excessively low-level cyber events).
[145] *See generally supra* Part II.C.
[146] *See generally supra* Part II.C.
[147] *See generally supra* Part II.C.

namely by necessity[148] and proportionality.[149] However, it conflates the *jus ad bellum* and *in bello* aspects of the latter norm and fails to properly apply each individually.

States and commentators agree that proportionality is a well-established and authoritative principle in international law,[150] yet the contours of those norms are glossed over.[151] This is particularly clear in the DoD Manual as the United States pays only nominal credence to the separation.[152] Proportionality is guided generally by the notion that the means used to achieve a given objective must be balanced against the harm caused.[153] Beyond that, what does proportionality actually require? The norms—though related in purpose—are separate; the first, *ad bellum* proportionality, governs the process leading up to the use of

[148] As noted above, this Comment does not delve into the rich analysis surrounding the principle of necessity nor how the two norms born of the Caroline case interact with each other to restrict the aggressive tendencies of States in the conduct of international relations. *Cf. supra* text accompanying note 52. Suffice it to say here that, where proportionality deals with the means used, necessity is concerned with the effectiveness of such an action to counter the ongoing threat posed by the initiating use of force. *See, e.g.*, *New Twist supra* note 52.

[149] Rule 16.3.3.1, by reference to rule 1.11.5 ("Use of Force in Self-Defense") acknowledges that Charter Article 51 governs legal force in the cyber context, while preserving the inherent right of states to respond in self-defense. *See* LAW OF WAR MANUAL, *supra* note 1, at 37, 46-47, 991 (acknowledging that the United States is bound by the customary norms and to be legitimate, "it is generally understood that the defending State's actions must be necessary . . . [and] proportionate to the nature of the threat being addressed").

[150] *E.g.*, Franck, *supra* note 68, at 716 (noting that, in rendering decisions, a panoply of courts, tribunals, and arbitrators have relied on proportionality as a principle governing State's obligations international law).

[151] *See, e.g.*, Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places*, 51 NAVAL L. REV. 132, 134 (2005) (defining proportionality by analogy risks definitional creep).

[152] *See supra* text accompanying note 137. (Describing the U.S. cautions against conflating the *ad bellum* and *in bello* norms, but fails to clarify its distinct obligations pursuant to both).

[153] *E.g.*, Franck, *supra* note 68, at 721. In *Nicaragua* and elsewhere, the ICJ staked out the authority to determine, case-by-case, the sufficiency of the provocation supporting self-defensive action. *Id.*. However, the Court has failed to make the threshold "significantly more determinate by [an] opinion rendered. *Id.* at 721-22. Thus, the threshold warranting the choice to resort to responsive force is unclear in the kinetic context—and certainly more so, in the cyber domain. *Id.*

force, where the second, *in bello* proportionality, relates to the action itself.[154] The DoD Manual's internal limit on responsive action ignores this distinction and addresses only the *in bello* means-ends restriction.[155]

Jus ad bellum proportionality, governing the moment prior to forceful response, necessarily controls the State's *choice* to invoke self-defense.[156] In the first instance, the Charter-based normative framework assigns sovereignty over force to the Security Council as an independent check on a State's ability to escalate a conflict.[157] Likewise, customary international law reinforces that strong presumption within the Charter away from escalation via the *ad bellum* aspect of proportionality.[158]

The overly permissive term used by the DoD Manual encapsulates a series of rights and obligations, which should only be employed in response to a sufficiently grave precipitating force.[159] "A likely—and unfortunate—effect of this expanded rhetoric will be to ease the threshold for characterizing an armed attack in the cyber arena, which correspondingly weakens the

---

[154] See *supra* text accompanying note 65.

[155] *See* LAW OF WAR MANUAL, *supra* note 1, at 991 ("There is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality."). 16.3.3.2 cites the Department of State Legal Advisor as authority for the proposition. *See also Koh*, *supra* note 23, at 374 ("There is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response . . . such responses must still be *necessary* and of course *proportionate*.").

[156] Johann Wolfgang Textor, *Synopsis Juris Gentium*, The Classics of International Law Vol. II 167 (commentating on a *casus belli* as a formality necessary towards the declaration of war, Johann Wolfgang Textor emphasized the justification precipitating the recourse to conflict); James Brown Scott ed., 1916, John Pawley Bate, trans. ("For recourse must not be had to war on any promiscuous ground for a slight hurt. . . . He, then, who is not really hurt, or only moderately, has no just cause of war.").

[157] *See supra* text accompanying note 29 (articulating the supremacy of the Security Council in authorizing uses of force by victim-States responsive to action below the threshold constituting an armed attack).

[158] *See supra* text accompanying note 65 (stating that the restrictions imposed by proportionality on the choice of response available to States).

[159] *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

prohibition against the use of force."[160] In a field such as cyber, where the low-level boundary is so unclear, based upon the DoD Manual, the United States may potentially access an "attack" level right in response to a sub-force cyber event precipitating action.

The over-inclusive span of cyber activity that the United States could incorporate in its "illegal force" calculus violates *ad bellum* proportionality.[161] The low-level gravity of the OPM hack, for instance, is insufficient to invoke self-defense.[162] Should the United States respond outright according to the DoD Manual, the disparity between the harm caused and the cyber attack threshold, which properly gives rise to the inherent right to use force, would be so disparate as to violate *ad bellum* proportionality.[163]

Moreover, if a State engages disproportionately in the *ad bellum* sense, where the precipitating event fails to meet the required threshold, then the *in bello* act will necessarily violate the norm as well.[164] *In bello* proportionality is somewhat clearer as a controlling theory of international law in that it is based on the

---

[160] *See Cyberwar Versus Cyber Attack*, *supra* note 21, at 94. The word "attack" has a particular legal meaning that triggers a permissive authority to respond in self-defense. *Id.* (characterizing the initial action is necessary to the permissibility of a self-defensive response). Precipitating force must surpass this threshold to trigger a State's inherent right to self-defense. Nicar. v. U.S., 1986 I.C.J. at 195 (predicating self-defense as a response to an "armed attack").

[161] *Compare supra* text accompanying note 129 (regarding the permissive calculation potentially available to the U.S.), *with supra* text accompanying notes 65, 156 (clarifying that *ad bellum* proportionality controls the choice of response).

[162] It is far from clear, at this stage, what the long-term effects of the OPM hack will be, or the intent of those responsible for the intrusion. Thus far, the United States does not appear to have incurred even the kind of political coercion that the *Nicaragua* Court determined as violative of State sovereignty. *Cf.* Nicar. v. U.S., 1986 I.C.J. at 108, para. 205. Thus, the OPM hack fails to qualify even as a use of cyber force, let alone as sufficient to trigger self-defense, per Article 51. *Cf. id.*

[163] *See* Kretzmer, *supra* note 63, at 240. Regardless of the *in bello* methods used, the choice to respond outright constitutes the violation of *ad bellum* proportionality. *Id.* "Use of force may be disproportionate under *jus ad bellum* even if all forcible measures are compatible with *jus in bello* in general, and the proportionality principle in *jus in bello* in particular." *Id.*

[164] *Cf.* Larry May, *The Nature of War and the Idea of "Cyberwar," in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 3, 15 (Jens David Ohlin et al. eds., 2015) ("Nearly all armed action taken as a countermeasure to a sub-armed attack is very likely to be considered disproportionate.").

relative quality of destruction between the initial action and the countermeasure, and so offers a more calculated constraint on States' responsive action.[165] However, the legality of proportionate action *in bello* hinges upon the relationship between the means deployed and the military objectives sought.[166]

Nothing in the DoD Manual precludes forceful responsive action to a low-level cyber event if the United States determines that the initial event is an illegal use of force.[167] Thus, if the United States took per se responsive forceful action, even a non-kinetic use of cyber force such as a Stuxnet-like virus, it would run counter to the *in bello* principle of proportionality.[168] The long-term outcome of the OPM hack is unclear,[169] and it is possible that the hack was a precursor to a more destructive action yet to come.[170] However, based on information currently available, the OPM hack certainly does not meet the threshold of an armed attack since it resulted only in the unauthorized access by the Chinese government to information held by OPM. .[171] As such, where the United States invokes a right to kinetic action based upon such a low-level precipitating event, that expansive gap between those

---

[165] The calculus of proportionality in conflict is better understood conceptually, and a majority of States—including the United States—rely more upon this principle in determining legitimate responsive action. *See* Franck, *supra* note 68, at 715, 723-24 (providing the example of A doing X to B, and B responding with Y, proportionality is concerned with whether response Y is "equivalent" to X).

[166] *Id.*

[167] *See* LAW OF WAR MANUAL, *supra* note 1, at 991. The DoD Manual expressly rejects any requirement to limit the United States to an in-kind response. *See id.* ("There is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.").

[168] *See supra* text accompanying note 69 (responding forcibly to a non-use of force constitutes a forceful reprisal); *Cf.* May, *supra* note 164, at 15.

[169] *See, e.g.*, Henry Farrell, *The hack on the U.S. government was not a 'cyber Pearl Harbor' (but it was a very big deal)*, WASH. POST, June 15, 2015, https://www.washingtonpost.com/news/monkey-cage/wp/2015/06/15/the-hack-on-the-u-s-government-was-not-a-cyber-pearl-harbor-but-it-was-a-very-big-deal/?utm_term=.1d803e8dde50.

[170] *See The OPM Hack*, *supra* note 92 (debating the severity of the hack in the context of the DoD Manual).

[171] It is worth noting that, as far as is known, no physical damage or death is directly attributable to the OPM hack, and so it does not meet the standard laid out by the DoD Manual. *Cf.* LAW OF WAR MANUAL, *supra* note 1, at 988-89.

thresholds may be deemed so great as to constitute a forceful reprisal.

IV. RECOMMENDATIONS

The remedy to the above issues is both domestic and international in nature. First, the United States should undertake a concerted reevaluation of its obligations under international law, both Charter-based and customary. Concurrently, the United States should work to clarify the rights and obligations of States in the cyber domain through the treaty-making process. Barring such reevaluation and clarification, the United States should develop and strengthen customary norms pertaining to cyber via the ICJ either through an advisory opinion[172] or by accepting jurisdiction in a contentious case.[173]

A. U.S. Policy Should Incorporate Definitional Precision

The United States should revise its overly permissive definition regarding what is sufficient to invoke self-defense. By limiting its definition regarding what constitutes certain levels of force and the concomitant rights of response, the United States will reduce the risks inherent in its current position. This will support

---

[172] Per the ICJ Statute, only States may directly refer cases to the Court. *See* Statute of the International Court of Justice. art. 38 art. 35. However, INT'L CT. JUST. art. 65 and U.N. Charter art. 96, para. 1 hold that competent organs of the U.N. may refer questions of law to the Court for advisory opinions. Statute of the International Court of Justice art. 65, para. 1 ("The Court may give an advisory opinion on any legal question at the request of whatever body may be authorized by or in accordance with the Charter of the United Nations to make such a request."); U.N. Charter art. 96, para. 1 ("The General Assembly or the Security Council may request the International Court of Justice to give an advisory opinion on any legal question."). Moreover, the General Assembly is competent in any case to refer questions pertaining to peace and security, and the codification of norms, to the Court. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 para. 11 (July 8).

[173] Pursuant to Article 36 of the ICJ Statute, the Court may only hear cases brought before it by States that have accepted its jurisdiction to adjudicate the merits of a case. Statute of the International Court of Justice art 36, para. 1 ("The jurisdiction of the Court comprises all cases which the parties refer to it and all matters specially provided for in the Charter of the United Nations or in treaties and conventions in force.").

the purpose of the U.N. Charter, underscoring the strong presumption away from force escalation. Moreover, such a reevaluation of policy will support the strategic interests of the United States in contributing to the establishment of international norms.[174]

The current DoD Manual fails to elucidate the contours of U.S. rights and obligations in the cyber context. While the Tallinn Manual is more closely aligned with the gradations set out in the Charter and *Nicaragua*, it is also too limited in scope as it neglects to address the ambiguous lower-bound threshold on force. Even if the United States wishes to maintain a greater level of flexibility by having more broadly encompassing definitions, it should do so, not by having a single, over-broad "right," but by delineating specific sets of actions that give rise to certain thresholds. Thus, the United States should clarify both the scope of precipitating events giving effect to *Nicaragua* and the Charter as well as create specific terms for acts below use of force.

Building the lexicon of U.S. definitions in the cyber context will effectuate the DoD Manual's assertion that both aspects of proportionality govern responsive action.[175] Rather than using the conflated norm, the United States should explicitly enforce the *ad bellum* aspect of proportionality by codifying the upper and lower bounds of use of force. This will in turn restrict the availability of per se responsive action and better control proportional decision-making processes. Doing so will minimize the risk that the United States' calculus will encompass an impermissibly broad span of acts, thus limiting risks of violating *ad bellum* and *in bello* proportionality.

---

[174] Norms develop through State practice and *opinio juris*, so if the United States were to implement a clearer set of definitions, and policies in support of specific thresholds, it would be more in line with the Tallinn Manual's interpretation of customary law. *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 354-55 (2015) [herineafter *The Cyber-Law of Nations*] (explaining that governing legal norms develop more easily than treaty law, partially through policy declarations by states).

[175] *See Cyberwar Versus Cyber Attack*, *supra* note 21 at 95 ("Using the term 'cyber attack' to describe acts that fall short of or outside the definition of attack . . . risks conflating . . . authorities and [legal] obligations.").

The United States should carefully craft precise but internationally cohesive terms.[176] First, the United States should retire the position that it may respond to "any illegal use of force"[177] and solidify the distinction between cyber force and cyber attacks. Second, the United States should more closely examine international definitions and attempt to fashion its own terms with regard to the cyber force spectrum, which reinforce other States' understanding of the norms.[178] Doing so will have the added benefit of reducing the risk that the United States may act impermissibly in response to substantially low-level cyber activity while bolstering customary norms below the use of force threshold through coherent State practice and *opinio juris*.[179]

As a remedy, a reevaluation of the U.S. position has the fewest obstacles because no international agreements will be necessary. Thus, the United States should undertake this review and supplement the DoD Manual with more precision as soon as possible, perhaps as an annex to the current DoD Manual. Most importantly, doing so will bring the United States back within the orbit of its responsibilities as a Member of the U.N. to support that organization's mission and purpose, including its prohibition on the use of force.

B. The United States Should Develop International Cyber Norms

Signing and ratifying an international agreement concerning the use of force in the cyber context would offer the

---

[176] The proliferation of sometimes-contradictory terms to describe rights within the cyber context has added greatly to the legal ambiguity currently governing operations in that domain. *Cf.* Phillip Pool, *War of the Cyber World: The Law of Cyber Warfare*, 47 INT'L L. 299, 308 (2013) (noting that, without cohesive terms, States have individually developed internationally contradictory definitions).

[177] *See* LAW OF WAR MANUAL, *supra* note 1, at 991.

[178] For instance, the Council of Europe's Convention on Cybercrime draws its terminology regarding lower-level cyber activity from the criminal sphere, and thereby reduces the opportunity for misapplication or confusion. *See* Watkin, *supra* note 125, at 504-05 (emphasizing that certain terms of art, like "attack," were not included in the convention text, but rather in the explanatory report).

[179] *See* Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 572 (2011) (defining *opinio juris* as conduct carried out by a State "out of a sense of legal obligation").

strongest assurance of compliance. Under international law, a treaty carries the most weight and is generally the clearest expression of international rights and obligations.[180] However, considering the general lack of consensus as to what State practice should be, finalizing a treaty on the matter is unlikely in the near future.[181] Moreover, the treaty-making process can be exceptionally prolonged, so the lack of current consensus does not bode well for a timely agreement as to State obligations.

Unlike treaty law, customary law does not require the explicit acceptance of States and may become binding based on the density of State practice at a much faster rate.[182] Thus, barring an international treaty, the United States should accept and implement the reasoning of the ICJ's threshold analysis from *Nicaragua*, at least so far as cyber is concerned. The United States should empower the ICJ to clarify cyber norms through one of two potential avenues. First, the United States should work through the General Assembly to request an advisory opinion from the ICJ, similar to *Nuclear Weapons*. There, the General Assembly sought clarification as to the legality of deploying nuclear weapons based not on the weapon itself but rather on the effects or scale of a

---

[180] As with other areas of international law, binding States to certain behavior in the cyber domain via the treaty process will settle the norms of a domain in a concrete way. *See* Mario Prost, 39 HOUS. J. INT'L L. 285, *Hierarchy and the Sources of International Law: A Critique*, 293, 300 (discussing the dominance of the treaty-primacy theory regarding sources of international law, noting the pragmatic value of express obligations agreed to by states); *see also The Cyber-Law of Nations*, *supra* note 174, at 354-55 ("[T]reaties enshrine a formal legal agreement about governance of [the cyber] domain. The high seas, outer space, and Antarctica all came to be governed by multilateral treaties, but so far cyber largely is not.").

[181] States do not currently agree upon the governance model that should be applied to the cyber domain: China and Russia have proposed State-centric governance structures, while the United States and its allies support a multi-stakeholder structure. *Id.* at 346. Specific to the use of force issue, as exemplified by the contrast between the DoD and Tallinn Manuals, many States define operative terms differently, leading to difficulty in completing a treaty governing cyber operations. *See* Pool, *supra* note 176, at 309 (identifying definitional differences between States as a major obstacle towards the establishment of a governing legal framework for the cyber domain).

[182] *See The Cyber-Law of Nations*, *supra* note 174, at 361 ("Unlike a treaty, which requires broad agreement and may take years to negotiate, norms can arise through states acting individually, bilaterally, regionally, or multilaterally and without agreement of all states.").

nuclear fallout. The court could likewise review the cyber issue on similar grounds, as a potential weapon deployable in the conduct of international force or aggression. Doing so is one avenue by which the court may clarify the applicability of customary thresholds established in *Nicaragua* to the cyber context.

Alternatively, the ICJ could issue a decision in a contentious case, as with the *Nicaragua* decision. Assuming that all concerned parties accepted the jurisdiction of the court to adjudicate such a matter, Iran could petition the ICJ to review the legality and determine liability regarding the Stuxnet virus. Assuming that the ICJ found the damage caused by Stuxnet attributable to the United States and Israel, the court could essentially re-issue its *Nicaragua* holding in the context of cyber norms. Although not directly binding on any other States, but instead those party to the decision,[183] the ICJ could again elucidate the contours of the prohibition on the use of force as it did in *Nicaragua*. In this instance, where all parties accept the jurisdiction of the court to adjudicate the merits, the ICJ could extend its reasoning to include both the customary norms that formed the basis of its 1986 *Nicaragua* decision, while also linking the reasoning more explicitly to the Charter-based prohibition. Short of a treaty, a decision on a contentious case, based explicitly on Charter-based obligations, offers the most binding option (for the parties involved) towards the establishment of clearer cyber norms.

By seeking out clarification from the ICJ, either through the General Assembly and an advisory opinion, or as a party to a contentious case, the United States could help develop international norms. This will bolster the U.S. goal of developing cyber norms and thus promote stability by further settling the law of the cyber domain. This would count as an achievement both of

---

[183] *See* Statute of the International Court of Justice art. 59. Technically, decisions of the Court are only binding on those States party to a given case. *Id.* ("The decision of the Court has no binding force except between the parties and in respect of that particular case."). Since Advisory Opinions, by definition, do not deal with contention between State parties, such decisions are not binding per se. *Cf. id.* However, such advisory opinions carry substantial weight, as evident by the longevity of the Nicaragua decision. *E.g.*, Julie Calidonio Schmid, *Advisory Opinions on Human Rights: Moving Beyond a Pyrrhic Victory*, 16 DUKE J. COMP. & INT'L L. 415-16 (2006).

domestic policy as well as in extending a more effective rule of law to cyber operations. Similar to the codification of precise definitions domestically, engaging in this process towards the growth of customary law in the cyber domain implicitly bolsters the purpose of the U.N., and it reinforces the sovereignty of the Security Council over lawful force by limiting an individual State's claims to per se responsive action.

V. CONCLUSION

As a leading international lawyer recently noted regarding the role of the U.S. Military in cyberspace, defining the threshold that permits a State to respond to force is a fundamentally legal question—it will be answered by policy.[184] If the DoD Manual, as it stands now, represents that policy in the cyber context, it does not comply with the international legal obligations of the United States. Undoubtedly, cyber operations are relatively new, and the international legal norms surrounding that domain are in flux and customary norms are as yet unsettled. Thus, States must interpret their obligations as applied to cyber based on a legal framework developed well before the birth of that domain.

By design, however, that framework is insufficiently flexible to absorb the complexities of new technologies. As such, the U.S. policies must comport to those legal norms. However, given the current ambiguities in the field, the United States should use a clearly established lexicon in the cyber domain, since those definitions have legal consequences. Thus, the United States should take effective measures to restrict its access to the "inherent right" to self-defense in response to uses of cyber force that do not constitute an armed attack. Doing so will adhere to the sovereignty of the Security Council governing the legal use of force as well as comply with the customary *jus ad bellum* requirement of proportionality. Such a policy restriction, based on a legal reinterpretation by the United States, will greatly reduce the likelihood that the United States will commit a forceful reprisal and thus violate *jus in bello* proportionality should it choose to respond to a low-level cyber event such as the OPM hack.

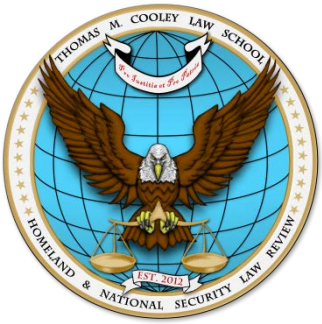
---

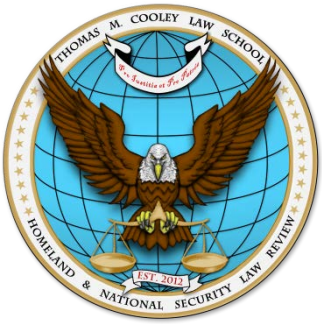
[184] Rishikof, *supra* note 18.

Likewise, on an international level, the United States should promote the clarification of the normative framework vis-à-vis cyber to help develop international customary law in that domain. Spearheading a treaty process will create an internationally binding framework and thus a particularly weighty obligation under international law. Barring that, the United States, through the General Assembly, may seek an advisory opinion from the ICJ, expounding its analysis in *Nicaragua* to explicitly address cyber norms. Alternatively, should Iran bring a contentious case before the Court seeking recourse for the 2010 Stuxnet virus, the United States (and Israel) should accept the jurisdiction of the ICJ to adjudicate the merits of that case. Doing so would develop international jurisprudence regarding threshold norms in the cyber context.[185]

As it stands now, the United States is vulnerable to accusations of non-compliance under international law regarding cyber operations. As both a matter of Charter-based and customary international law, the DoD Manual poses significant problems regarding compliance. Particularly given the current state of customary cyber law, the United States should be explicit in its definitions and cognizant of the potential legal consequences. The 2015 DoD Manual worsens these issues, and U.S. policy should be clarified to comply with States international legal obligations pertaining to the prohibition on force.

[185] The decision of the ICJ would be binding only upon the parties to the decision, but by publicizing its reasoning and decision coming out of a Stuxnet Virus-based case, the Court would broadcast its interpretation and clarify Nicaragua vis-à-vis cyber. *See supra* text accompanying note 183 (regarding the weight of the ICJ's interpretations towards the development of customary norms).


THOMAS M. COOLEY LAW SCHOOL
HOMELAND & NATIONAL SECURITY LAW REVIEW
EST. 2013



NATIONAL SECURITY LEAKS, THE ESPIONAGE ACT, AND PROSECUTORIAL DISCRETION

David J. Ryan

I. INTRODUCTION

Throughout its history, the U.S. government has often sought to deter and punish the unauthorized disclosure of national security information.[1] During World War I, Congress passed the Espionage Act of 1917,[2] providing the Executive Branch a powerful tool to achieve those ends. The Act, which exists in much the same form today,[3] imposes harsh criminal sanctions on those who reveal the nation's most vital secrets to its adversaries.[4] However, the Act's reach extends well beyond this traditional conception of espionage, enabling criminal prosecutions that are significantly more controversial. In particular, the Act may be applied to individuals who leak sensitive information to the news

[1] *See* Erin Creegan, *National Security Crime*, 3 HARV. NAT'L SEC. J. 373, 390-91 (2012) (describing the history of U.S. espionage prosecutions).
[2] The Espionage Act, 18 U.S.C.A §§ 792-799 (Westlaw 2017).
[3] *See* Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 221 (2007).
[4] *See* 18 U.S.C.A. § 793(f) (providing that the statutory maximum penalty for an Espionage Act violation is ten years of imprisonment).

media, even when they do so to expose misconduct by the government or to foster debate on important public policies.[5]

The use of the Espionage Act in leak prosecutions is a relatively novel development.[6] Prior to the Trump administration, the Department of Justice (DOJ) had prosecuted only twelve leak cases under the Act, and most of those took place after the inauguration of President Obama in 2009.[7] Indeed, the Obama administration initiated or continued Espionage Act prosecutions against eight leakers, far more than any other administration.[8] Moreover, some of its prosecutions employed investigative methods that encroached on the media's non-public records and communications, prompting intense criticism and fears of a crackdown on freedom of the press.[9] In an effort to address these concerns, the Obama administration published policy guidance in 2014 that substantially limited the ability of federal law enforcement to investigate members of the news media.[10] Although this guidance addressed some of the media's concerns,[11] it did not explain the administration's general policy regarding the prosecution of leakers. Critics continue to argue that the

---

[5] *See, e.g.*, Complaint, United States v. Snowden, No. 1:13-CR-265 (CMH) (E.D. Va. June 14, 2013), https://fas.org/sgp/jud/snowden/complaint.pdf (charging Edward Snowden under the Espionage Act for leaking sensitive details concerning National Security Agency (NSA) surveillance programs to the press).

[6] *See* Katherine Feuer, *Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act*, 38 B.C. INT'L & COMP. L. REV. 91, 98 (2015) (describing 2009 as the "turning point" when the executive branch began to enforce the Espionage Act against leakers).

[7] *Id.* at 99-104 (describing the ten prosecutions of leakers since 2006).

[8] *Id.*

[9] *See* Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 450 B.U. L. REV. 449, 451-53 (2014).

[10] Memorandum from Att'y Gen. to All Dep't Emps., *Updated Policy Regarding Obtaining Info. from, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media* (Jan. 14, 2015) [hereinafter Att'y Gen. Memo], https://fas.org/sgp/othergov/doj-media-rev.pdf.

[11] For example, the policy guidance requires Attorney General approval to apply for a warrant to search the premises of a news media organization or to question a member of the news media for any suspected offense arising out of her newsgathering activities. *See id.*; U.S. DEP'T OF JUSTICE, U.S ATTORNEYS' MANUAL § 9-13.400 (1997, rev. ed. Oct. 2016) [hereinafter U.S ATTORNEYS' MANUAL].

government's enforcement approach is arbitrary[12] and does not account for the fact that leaking is commonplace and widely tolerated within the national security bureaucracy.[13] Others characterize many leak prosecutions as punishing good-faith disclosures of government misconduct with little attendant benefit to national security.[14]

Such criticism has led to further demands to limit the DOJ's ability to prosecute leakers.[15] Many reform advocates focus on the text of the Espionage Act itself, which had been widely disparaged for its ambiguity and incoherence well before the Obama administration.[16] Their statutory reform proposals include, *inter alia*, changing the Act's scienter requirement, reducing liability for certain categories of leakers, and revising the Act's definition of national defense information.[17] Other reform advocates would pursue non-legislative methods, such as relying on security technology instead of law enforcement to prevent leaks or encouraging the judiciary to impose more stringent requirements on leak prosecutions.[18]

This Note proffers an analytical framework for the prosecutor who is considering whether to enforce the Espionage Act against a national security leaker. If adopted as executive branch policy, the proposed framework would address some—

---

[12] *See* David McCraw & Stephen Gikow, *The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World*, 48 HARV. C.R.-C.L. L. REV. 473, 487 (2013).
[13] *See* David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 528 (2013).
[14] *See* Mary-Rose Papandrea, *National Security Information Disclosures and the Role of Intent*, 56 WM. & MARY L. REV. 1381 (2015).
[15] *See, e.g.*, T.S. Ellis, III, *National Security Trials: A Judge's Perspective*, 99 VA. L. REV. 1607, 1624 (2013); Nathan Alexander Sales, *Can Technology Prevent Leaks?*, 8 J. NAT'L SECURITY L. & POL'Y 73 (2015); Pamela Takefman, *Curbing Overzealous Prosecution of the Espionage Act: Thomas Andrews Drake and the Case for Judicial Intervention at Sentencing*, 35 CARDOZO L. REV. 897 (2013).
[16] *See* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 930 (1973) ("[T]he [Espionage Act] implacably resist[s] the effort to understand.").
[17] *See, e.g.*, Ellis, *supra* note 15; Takefman, *supra* note 15.
[18] *See, e.g.*, Sales, *supra* note 15.

though not all—of the concerns voiced by critics of the Obama administration's enforcement approach. The framework, moreover, is largely consistent with the DOJ's recent use of the Espionage Act in leak prosecutions. Indeed, the framework's primary objective is to adapt the DOJ's longstanding general policy for commencing or declining prosecution[19] to the special context of prosecuting national security leaks. To that end, the framework is comprised of five critical factors for prosecutors to consider when deciding whether an Espionage Act prosecution is the appropriate response to a national security leak:

> 1. Whether the leaked information was properly classified such that its disclosure caused *actual* harm to U.S. national security interests;
>
> 2.Whether the putative defendant was obligated to safeguard classified information due to his or her employment;
>
> 3.Whether the putative defendant, regardless of motive, reasonably should have known that the leak could harm U.S. national security or benefit a foreign power;
>
> 4.Whether the putative defendant held a high-ranking government position; and
>
> 5.Whether prosecution would threaten to disclose additional classified information.

This Note applies these factors to several real-world and hypothetical leak cases, illustrating how they provide appropriate guideposts for the exercise of prosecutorial discretion in this context. It additionally explains why these factors are consistent with the DOJ's general policy of initiating prosecution when there is sufficient evidence to obtain a conviction and where a "substantial federal interest would be served," unless the defendant can effectively be prosecuted elsewhere or "there [is] an adequate non-criminal alternative to prosecution."[20]

---

[19] *See* U.S ATTORNEYS' MANUAL, *supra* note 11, § 9-27.220.
[20] *See id.*

In other specialized contexts, such as the prosecution of business organizations, the DOJ has promulgated comparable factors to implement its general enforcement policy.[21] However, it has not yet done so for the prosecution of national security leakers. This Note accordingly concludes by advocating for the DOJ to adopt the framework's factors into its official policy guidance for prosecutors, explaining why such a reform measure is both viable and likely to address many concerns associated with the prosecution of leakers under the Espionage Act.

II. BACKGROUND

It is first necessary to provide an overview of 18 U.S.C. §§ 793(d) and 793(e), the two Espionage Act provisions most applicable to national security leaks. The provisions are essentially identical, except that § 793(d) applies to individuals who were "entrusted with" or "lawfully . . . possess[ed]" the leaked information, whereas § 793(e) applies to "unauthorized" possessors.[22] These provisions criminalize national security leaks by prohibiting the "willful" disclosure of information "relating to the national defense" to any person "not entitled to receive it."[23] The Act provides no guidance on what constitutes "national defense" information, but subsequent case law indicates that the term encompasses most information concerning the military and "related activities of national preparedness," regardless of whether disclosure actually harms national security.[24] Although leak prosecutions under the Espionage Act typically involve classified information,[25] the Act predates the modern classification system, and there is no requirement for national defense information to be classified.[26] Moreover, while courts have construed the Act to preclude prosecuting a leak of information that is already in the public domain or a leak of improperly concealed government

---

[21] *See id.* § 9-28.300.
[22] 18 U.S.C.A. § 793 (Westlaw 2017).
[23] *Id.*
[24] *See* Gorin v. United States, 312 U.S. 19, 28 (1941).
[25] *See* Feuer, *supra* note 6, at 99-110 (listing leak prosecutions involving classified information).
[26] JENNIFER K. ELSEA, CONG. RESEARCH SERV., R41404, CRIMINAL PROHIBITIONS OF THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 9 (2013).

information, they also tend to defer to the Executive Branch's judgment on these issues.[27]

With respect to the Act's scienter requirement, it has long been understood that §§ 793(d) and (e) tacitly distinguish between leaks of tangible and intangible information.[28] Both provisions require the government to prove that the leaker acted "willfully" or "with knowledge that [his or her] conduct was unlawful."[29] However, for leaks of intangible information, which is typically transmitted orally, in contrast to tangible leaks of documents or photographs, the government must also prove that the defendant had "reason to believe [the information] could be used to the injury of the United States or to the advantage of any foreign nation."[30] The precise meaning of the additional scienter requirement for intangible information is unsettled, but it does not clearly require proof of a defendant's specific intent to harm U.S. national security or benefit a foreign government.[31]

By its terms, the Espionage Act criminalizes many, if not most, of the countless leaks that are "a routine method of communication" by members of the government.[32] Moreover, a conviction under the Act results in severe criminal penalties. The maximum sentence for violating §§ 793(d) or (e) is ten years' imprisonment,[33] and the U.S. Sentencing Guidelines recommend a sentence of 97 to 121 months for an offender with no criminal history who is convicted of violating either provision.[34] A sentence of this magnitude may be appropriate for the senior political official who compromises a valuable U.S. intelligence source by selectively leaking information to influence a partisan debate. Such a penalty, however, may not be warranted for the low-level government employee who exposes waste and abuse within a defense program without causing any perceptible impact on national security. Another reason for caution is the prospect of

---

[27] *Id.*
[28] *See* Edgar & Schmidt, *supra* note 16, at 966-67.
[29] United States v. Hitselberger, 991 F. Supp. 2d 101, 107 (D.D.C. 2013).
[30] 18 U.S.C.A. § 793(d)-(e) (Westlaw 2017).
[31] *See* Papandrea, *supra* note 14, at 1384 n.8.
[32] Pozen, *supra* note 13, at 528.
[33] 18 U.S.C.A. § 793(f).
[34] U.S. SENTENCING COMM'N, GUIDELINES MANUAL § 2M3.2 at 291-92, 420 (Nov. 2016).

"graymail," which occurs when a criminal defendant threatens to introduce classified evidence as part of his or her defense.[35] Although a leak prosecution involves sensitive information that has already been disclosed publicly, an accused leaker typically knows of other classified information that has not yet been disclosed, making the risk of graymail particularly acute.[36]

III. THE FRAMEWORK

One of the principal justifications for prosecutorial discretion is that criminal statutes tend to be overbroad, authorizing prosecutions that are outside the contemplation of the enacting legislature.[37] This concern is especially relevant to leak prosecutions under the Espionage Act, since Congress's apparent goal in enacting the statute was to criminalize the disclosure of state secrets to foreign adversaries, not the news media.[38] As the subsequent discussion indicates, leak prosecutions under the Act present various other doctrinal and practical problems, heightening the need for informed prosecutorial discretion. To that end, DOJ lawyers should consider the following factors when determining whether a leak prosecution will further the government's critical interest in protecting state secrets while minimizing the risk of harm to other important interests and constituencies.

---

[35] *See* Afsheen John Radsan, *Remodeling the Classified Information Procedures Act (CIPA)*, 32 CARDOZO L. REV. 437, 446 (2010).

[36] *See, e.g.*, Charlie Savage, *For U.S. Inquiries on Leaks, a Difficult Road to Prosecution*, N.Y. TIMES (June 9, 2012), http://query.nytimes.com/gst/fullpage.html?res=9F0DE4DF1739F933A25755C0A9649D8B63 ("Defendants [in leak prosecutions] who choose to fight often rely on a so-called graymail defense. This involves making the disclosure of further classified information a centerpiece of their right to a fair trial by pushing for even more revelations, such as identifying other people at the agency who had access to the same knowledge.").

[37] Stephanos Bibas, *The Need for Prosecutorial Discretion*, 19 TEMP. POL. & CIV. RTS. L. REV. 369, 369 (2010).

[38] Lindsay B. Barnes, *The Changing Face of Espionage: Modern Times Call for Amending the Espionage Act*, 46 MCGEORGE L. REV. 511, 512-13 (2014).

A. Whether the Leaked Information Was Appropriately Classified Such That Its Disclosure Caused Actual Harm to U.S. National Security Interests

In general, national security leaks disclose information that is subject to the Executive Branch's classification policies.[39] The fact that leaked information is classified, however, is only necessary, not sufficient, to justify a prosecution under the Espionage Act. Given the frequency of leaking, the prevalence of improper and excessive classification, and the availability of alternative sanctions for leaks of lesser importance, the DOJ's limited enforcement resources should be addressed to the most significant leaks that actually harm U.S. national security.[40]

Information becomes classified when a senior executive branch official determines that its disclosure could reasonably be expected to harm national security.[41] Many critics have noted that these determinations are highly arbitrary and that even reasonable classification decisions often result in pervasive "overclassification."[42] For instance, lower-level employees within the national security bureaucracy must apply the classification guidance of senior officials to every document, presentation, and email they create, a practice known as "derivative classification."[43] Facing severe penalties for under-classification and effectively no consequences for over-classification, these employees inevitably err on the side of treating information as classified.[44] Moreover, the Executive Branch typically classifies information for a default period of at least ten years and, in many cases, for significantly longer.[45] While it is possible to petition for earlier declassification

---

[39] *See* Exec. Order No. 13526, 75 Fed. Reg. 707, 707-08 (Jan. 5, 2010).
[40] *See* Radsan, *supra* note 35; Savage, *supra* note 36; Bibas, *supra* note 37; Barnes, *supra* note 38.
[41] *See* Exec. Order No. 13526, 75 Fed. Reg. at 707-08.
[42] *See, e.g.*, Alexander M. Taber, *Information Control: Making Secrets and Keeping Them Safe*, 57 ARIZ. L. REV. 581, 583-84 (2015) (listing critics); *see also National Security Leaks and the Law: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 34-35 (2012) [hereinafter Vladeck Statement] (statement of Prof. Stephen Vladeck).
[43] *See* Taber, *supra* note 42, at 584 n.15.
[44] *See* Pozen, *supra* note 13, at 592-94.
[45] *See* Exec. Order No. 13526, 75 Fed. Reg. § 1.5(b). The classification system makes certain exemptions to this default period. For instance, agencies are

if the information becomes public, or if disclosure would no longer pose any risk, in practice this occurs too infrequently to act as a significant check against overclassification.[46]

Given the significant risk of improper or excessive classification, the bare fact that information leaked to the media is classified is often insufficient to justify a criminal prosecution.[47] And even when leaked information was appropriately classified, the analysis supporting the classification decision was still conducted from an *ex ante* perspective, relative to the time of the leak, by projecting what harm *might* occur from improper disclosure.[48] With the benefit of an *ex post* perspective, the federal prosecutor should evaluate what harm *actually* resulted from disclosure and decline to prosecute when the prospective harm supporting the classification decision cannot reasonably be expected to occur. Instead, a leak prosecution under the Espionage Act should be predicated on a discrete, substantial harm to national security that is traceable to the leak.

In conducting this analysis, the prosecutor need not find that a leak indisputably caused the loss of life or the failure to achieve a military or diplomatic objective.[49] Rather, an enhanced risk of these consequences, or even lesser ones, may be sufficient to justify prosecution, particularly if the risk relates to a critical

---

expected to declassify information that "no longer meets the standards for classification," and are authorized in "exceptional cases" to disclose information "when the public interest in declassification outweighs the need to protect that information." *Id.* § 3.1; *see also* JENNIFER K. ELSEA, CONG. RESEARCH SERV., RS21900, THE PROTECTION OF CLASSIFIED INFORMATION: THE LEGAL FRAMEWORK 4-6 (2013) (citations omitted).

[46] *See* Papandrea, *supra* note 9, at 472-73.

[47] *See* Vladeck Statement, *supra* note 42, at 32-33, 37-38.

[48] *See* Exec. Order No. 13256, 75 Fed. Reg. § 1.2(a) (emphasis added) (defining Top Secret, Secret, and Confidential classification categories based on the extent to which unauthorized disclosure could reasonably "be *expected* to cause" harm to national security).

[49] *See* Ed Pilkington, *Bradley Manning Leak Did Not Result in Deaths by Enemy Forces, Court Hears*, THE GUARDIAN (July 31, 2013), https://www.theguardian.com/world/2013/jul/31/bradley-manning-sentencing-hearing-pentagon (explaining that a leak that caused these consequences would present the strongest justification for initiating prosecution).

U.S. interest.[50] Additionally, prosecutors evaluating the harm caused by a leak should consult with officials from the agency where the leaked information originated, since they are likely best positioned to assess the information's importance to the agency's mission and U.S. national security. Where possible, moreover, the prosecutor should also consult with a subject-matter expert from outside the originating agency to ensure that the information was not classified for impermissible reasons, such as concealing legal violations or embarrassing conduct by agency personnel.

Imposing these requirements would preclude Espionage Act prosecutions for leaks of inappropriately classified information and for leaks that do not cause actual harm to national security. Though such cases might have a sufficient legal and factual basis to proceed under the Act, the government's enforcement resources are best devoted to cases that are consistent with the national-security-harm-focused approach proposed here. While sanctions are still needed to punish and prevent leaks that fall short of causing such harm, that interest can often be satisfied through administrative actions, such as termination of employment or revocation of an individual's security clearance.[51]

Additionally, following the discretionary limits prescribed here will tend to increase the likelihood of a successful prosecution. Although the Espionage Act does not impose any requirement of proper classification or actual national security harm, judicial decisions in national security leak cases indicate that these factors bear on the outcome of each stage of the case. In *United States v. Kim*, for instance, the district court denied the defendant's motion to dismiss the indictment, while recognizing

---

[50] *Id*. For example, the U.S. government admitted that Bradley Manning's disclosure of large volumes of classified information did not result in a confirmed loss of life. *Id*. Notwithstanding this admission, Manning's judge sentenced her to 35 years of imprisonment, a sentence reflecting "the gravity of the case and the government's perception of the damage that was done." Charlie Savage & Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, N.Y. TIMES (Aug. 21, 2013), http://www.nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html.

[51] *See* Pozen, *supra* note 13, at 527 (describing how the loss of a security clearance effectively precludes one from working in the national security bureaucracy).

that he could "argue that the information he [was] charged with leaking was . . . not properly classified . . . as part of his defense" at trial.[52] In another case, *United States v. Morison*, the court's discussion of the national security harm caused by the defendant indicated that it weighed heavily against him in the court's consideration of his appeal. In affirming the defendant's conviction for selling classified satellite images to *Jane's Defense Weekly*, the U.S. Court of Appeals for the Fourth Circuit observed that the defendant "knew that he was dealing with national defense material which a foreign government . . . [could] use . . . either for itself, in following the movements of the agents reported upon, or as a check upon this country's efficiency in ferreting out foreign espionage."[53] Judge J. Harvie Wilkinson's concurring opinion similarly emphasized that the defendant's actions could have "hamper[ed] the effectiveness of expensive surveillance systems which would otherwise be expected to provide years of reliable information not obtainable by any other means."[54] Separately, once a convicted national security leaker appears for sentencing, it is undeniable that the degree to which the leak harmed national security is likely to play a critical role in the court's determination of the appropriate punishment.[55]

In short, even though the inquiries proposed here are not required as a formal matter, the prudent prosecutor must consider them in deciding whether to charge a national security leaker under the Espionage Act. By only enforcing the Act against those who leak properly classified information and cause actual harm to national security in doing so, the prosecutor both conserves enforcement resources and puts the case on a much stronger footing.

---

[52] United States v. Kim, 808 F. Supp. 2d 44, 55 (D.D.C. 2011).
[53] United States v. Morison, 844 F.2d 1057, 1073 (4th Cir. 1988) (quoting Gorin v. United States, 312 U.S. 19, 29 (1941)).
[54] *Id.* at 1082.
[55] *See, e.g.*, Transcript of Sentencing Hearing at 24, United States v. Sterling, No. 1:10cr485 (E.D. Va. 2015) (imposing a greater sentence on a defendant who leaked a clandestine source's identity because "there is in [the Court's] view no more critical secret than the secret of those people who are working on behalf of the United States in covert capacities").

B. Whether the Putative Defendant Was Obligated to Safeguard Classified Information Due to His or Her Employment

A national security leak typically occurs when a government employee or contractor provides classified information directly to the news media.[56] But some leaks happen indirectly—for instance, where a person lacking any official status conveys state secrets to the media after receiving them from a government insider.[57] Although the Espionage Act authorizes the prosecution of *any* individual who transfers national defense information to a party not entitled to receive it,[58] including those who leak indirectly, prosecutors should charge only those national security leakers who were entrusted with classified information in the course of their employment relationship with the government.[59]

The first reason for limiting leak prosecutions to government employees and contractors is to ensure that the defendant has sufficient culpability to justify a federal criminal case. Although any individual who leaks state secrets to the press is arguably culpable to some extent, those who do so while holding a position of public trust are far more blameworthy.

Another important reason for limiting leak prosecutions in this manner relates to the fact that government employees and contractors must fulfill various administrative requirements to access classified information. Most notable among these is the requirement to possess a security clearance, which one obtains by undergoing a background investigation and receiving a favorable

---

[56] *See* ELSEA, *supra* note 26, at 11 (defining leaks as "the release of classified information to persons without a security clearance, typically journalists").

[57] *See Constitutional Law—Due Process and Free Speech—District Court Holds That Recipients of Government Leaks Who Disclose Information "Related to the National Defense" May Be Prosecuted Under the Espionage Act.—United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006)*, 120 HARV. L. REV. 821, 822 (2007) (explaining how lobbyists for American Israel Public Affairs Committee were prosecuted for obtaining classified information from various government officials and then leaking it to others, including the media).

[58] The Espionage Act, 18 U.S.C.A §§ 792-799 (Westlaw 2017).

[59] Absent unusual circumstances, this category of people is limited to members of the military, civilian federal government employees, and government contractors. This Note uses the term "government employee" to refer to all three types of personnel.

evaluation of the investigation's results.[60] In addition, government employees must sign a non-disclosure agreement prior to accessing classified information, which imposes a lifetime contractual prohibition against unauthorized dissemination.[61] And even after receiving initial access to classified information, government employees must periodically complete training on security requirements and sign additional non-disclosure agreements when transferring between assignments.[62]

These administrative requirements play a critical role in defeating legal challenges to prosecutions of national security leakers. The clearest example of this is the judicial rejection of challenges based on the doctrines of vagueness and overbreadth, which are routinely invoked by Espionage Act defendants.[63] In a vagueness challenge, the defendant argues that the Act's text is too imprecise to give sufficient notice as to what conduct it prohibits, resulting in a deprivation of due process.[64] With an overbreadth challenge, the defendant contends that the Act's blanket prohibition of national security leaks by any individual excessively infringes on the public's First Amendment interests.[65] In rejecting both types of constitutional challenges, courts have relied on the government's procedures for granting security clearance and access to classified information. Since a vagueness challenge alleges that the defendant lacked adequate notice that his or her conduct was prohibited,[66] it cannot be made easily by a government employee who has signed a non-disclosure agreement and received training on the requirements for handling classified material. Similarly, limiting leak prosecutions to the class of persons who obtain sensitive information through their government employment substantially mitigates the problem of overbreadth.

---

[60] *See* ELSEA, *supra* note 45, at 7; *see generally* MICHELLE CHRISTENSEN, CONG. RESEARCH SERV., R43216, SECURITY CLEARANCE PROCESS: FREQUENTLY ASKED QUESTIONS (2016).
[61] *See* Sales, *supra* note 15, at 78.
[62] *See* CHRISTENSEN, *supra* note 60, at 1; *see also* Exec. Order No. 13526, 75 Fed. Reg. 707, § 4.1 (Jan. 5, 2010).
[63] *See, e.g.*, United States v. Rosen, 487 F. Supp. 2d 703, 710 (E.D. Va. 2007) (considering vagueness and overbreadth challenge); United States v. Morison, 844 F.2d 1057, 1070-73 (4th Cir. 1988).
[64] *Morison*, 844 F.2d at 1070-73.
[65] *Id.*
[66] *See id.* at 1072-73.

When the individual being charged for leaking is a government employee, as opposed to a member of the news media or other private individual, a leak prosecution is less likely to chill the exercise of free speech by the general public.

One final reason for limiting leak prosecutions to government employees and contractors is the Espionage Act's scienter requirement. This consideration is particularly important in cases involving leaks of intangible information, where a conviction requires proof that the defendant had reason to believe disclosure could harm the United States or benefit a foreign power.[67] In such cases, when the defendant has served in a sensitive position in the military or intelligence community, a factfinder can rely on that experience in concluding that the defendant was aware of the leak's potential impact on national security. As for leaks of tangible information, which only require proof that the defendant knew his or her actions were unlawful,[68] the administrative requirements discussed previously—in particular, the non-disclosure agreement and security training—prevent a defendant from claiming that he or she lacked such knowledge. Conversely, an accused leaker who has not been subject to these requirements can more plausibly argue that he or she did not know his or her actions were illegal.[69]

C. Whether the Putative Defendant Regardless of Motive, Reasonably Should Have Known That the Leak Could Harm U.S. National Security or Benefit a Foreign Power

The Espionage Act, like criminal statutes generally, does not require a particular motive for the defendant to be liable.[70] Rather, the Act sanctions all individuals who willfully disclose classified information that could reasonably be expected to harm national security or benefit a foreign power.[71] Thus, a defendant with the requisite mens rea is liable whether he or she leaks in order to expose government misconduct or to obtain a financial

---

[67] *See supra* notes 29-30.
[68] *Id.*
[69] *See* United States v. Rosen, 445 F. Supp. 2d 602, 634-35 (E.D. Va. 2006).
[70] *See* Carissa B. Hessick, *Motive's Role in Criminal Punishment*, 80 S. CAL. L. REV. 89, 90 (2006).
[71] *See supra* Part II.

reward. This is troubling to many observers who contend that individuals should not face criminal liability for leaking out of a good-faith belief that their actions are in the public interest.[72] The intense public controversies following Edward Snowden's NSA disclosures[73] and other recent national security leaks[74] suggest that these concerns are not without merit.

Nonetheless, prosecutors should limit their inquiry into the leaker's state of mind by focusing on whether he or she possessed the requisite mens rea under the Act and not on whether the leak might have had a salutary purpose. The first reason for this approach is that a less blameworthy motive does not mitigate the impact of a leak on national security. By way of example, there is broad agreement among current and former government officials that Edward Snowden's leaks caused catastrophic damage to vital U.S. intelligence capabilities and diplomatic interests.[75] The fact that Snowden's professed intention was to inform the public about the government's vast surveillance powers and the NSA's collection practices[76] did not mitigate, whatsoever, the harmful consequences of his actions.

Indeed, virtually all of the federal government's sensitive military and intelligence operations are potentially subject to criticism, even though they are shielded from public scrutiny to

---

[72] *See generally* Papandrea, *supra* note 14.

[73] *See, e.g.*, John Cassidy, *Why Edward Snowden Is A Hero*, NEW YORKER (June 10, 2013), http://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero (defending Snowden's disclosures and noting intense disagreement on this issue).

[74] *See, e.g.*, Lucy Wescott, *Chelsea Manning: 115,000 Sign Petition To Drop Charges Related To Suicide Attempt*, NEWSWEEK (Aug. 10, 2016, 2:58 PM), http://www.newsweek.com/chelsea-manning-suicide-attempt-charges-drop-489199 (describing outpouring of public support for convicted leaker Chelsea Manning).

[75] *See, e.g.*, Tony Capra, *Snowden Leaks Could Cost Military Billions: Pentagon*, NBC NEWS (Mar. 6, 2014, 5:27 PM), http://www.nbcnews.com/news/investigations/snowden-leaks-could-cost-military-billions
-pentagon-n46426.

[76] Barton Gellman & Jerry Markon, *Edward Snowden says motive behind leaks was to expose 'surveillance state,'* WASH. POST (June 10, 2013), https://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?utm_term=.a766a9f1aeac.

ensure their effectiveness. Ultimately, the decision to engage in activities such as electronic surveillance or covert action is the prerogative of the nation's elected leaders. A policy of tolerating leaks with purportedly worthy motives would effectively permit private individuals to usurp the authority of Congress and the President to make critical national security decisions on behalf of the country. Additionally, a policy of only targeting leakers who have a disfavored motive is likely to be unworkable in practice. Most leakers can plausibly claim that at least one of their motives was altruistic, and it may be impossible to establish with any certainty whether a defendant's professed motive is sincerely held.

Of course, motive is not entirely irrelevant to the exercise of prosecutorial discretion. As in any criminal case, the defendant's motive in a leak prosecution plays a critical role in the government's theory of the case—*i.e.*, the factual narrative underlying the charged offenses, including the reasons motivating the defendant's actions, and how that narrative is consistent with the available evidence. Motive, moreover, is likely to bear on the district court's determination of the leaker's sentence. Apart from these considerations, however, the framework proposed here emphasizes the harm resulting from the leaker's conduct and excludes the issue of his or her motive so long as the leaker has the requisite mens rea under the Espionage Act.

D. Whether the Putative Defendant Held a High-Ranking Government Position

Although liability under the Espionage Act does not depend on the defendant's seniority in government, there are several reasons for prosecutors to take this issue into consideration. The first is that it is incredibly difficult to detect and punish leakers. Only a small fraction of the countless leaks that occur each year are referred to law enforcement for further investigation.[77] In the majority of cases, the number of individuals who had access to the information and potentially could have leaked it is so large that an

[77] *See National Security Leaks and the Law: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 10-14 (2012) (statement of Kenneth Wainstein, Partner, Cadwalader, Wickersham & Taft LLP).

investigation is unlikely to reveal the leaker's identity.[78] Thus, the government must use the few leaks that can be prosecuted to achieve the greatest possible deterrent effect. Although deterrence of crime depends in part on the severity of punishment,[79] it also depends on the visibility of the crime's consequences to the population of potential offenders.[80] The prosecution of a senior official for leaking is likely to command the attention of lower-level employees within the national security bureaucracy. Moreover, it will demonstrate to lower-level employees that, if their superiors can be held accountable for leaking, then they are likely to face the same consequences.

Additionally, rank-and-file employees in the national security bureaucracy are more likely than senior officials to be deterred by non-criminal sanctions for unauthorized disclosures of classified information.[81] These sanctions include the loss of employment and revocation of security clearance[82]—consequences that disproportionately affect career bureaucrats and lower-level employees. This category of individuals, unlike senior political appointees who typically have alternative career opportunities outside the government, may never be able to obtain comparable reemployment without a security clearance.[83] Conversely, criminal prosecution may be the government's only effective recourse against a high-ranking leaker who would face relatively minor financial and professional repercussions from administrative sanctions.

Prosecutors should also consider the perceptions of illegitimacy and unfairness associated with an enforcement approach that imposes harsh criminal punishment on lower-level employees while shielding high-ranking officials. This issue

---

[78] *See id.*
[79] Hessick, *supra* note 70, at 112, 115-18.
[80] *Cf.* Liezl Walker, *The Deterrent Value of Imposing Prison Sentences for Tax Crimes*, 26 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 1, 26-27 (2000) (explaining how high-profile tax prosecutions of public figures achieve greater deterrence effects).
[81] *Cf.* Pozen, *supra* note 13, at 530 (explaining that "[m]ost bureaucrats have little to gain in their careers from leaking, and much to lose").
[82] *See* ELSEA, *supra* note 45, at 8.
[83] *Cf.* Takefman, *supra* note 15, at 905 (explaining how mid-level government officials targeted in leak prosecution face "financial ruin").

surfaced several years ago when the DOJ declined to bring Espionage Act charges against General David Petraeus for disclosing his classified personal notebooks to his biographer.[84] Instead, the DOJ permitted Petraeus to plead guilty to the misdemeanor offense of mishandling classified information.[85] Petraeus's defenders said this approach was warranted in light of his extraordinary record of public service and because his biographer did not actually publish the information in the notebooks.[86] However, these considerations did not prevent significant controversy over the DOJ's decision.[87] Many commentators criticized what they viewed as an unusually lenient outcome for the former Central Intelligence Agency (CIA) director—namely, a sentence of probation and a fine—and noted the disparity between his sentence and the lengthy prison terms received by more junior officials who also leaked classified information.[88]

The controversy played out in the courtroom as well. Defense attorneys for Jeffrey Sterling—a CIA officer convicted under the Espionage Act for leaking details about U.S. efforts to undermine Iran's nuclear program—repeatedly emphasized General Petraeus's lenient punishment as they defended Sterling.[89]

---

[84] *See, e.g.*, Adam Goldman, *How David Petraeus avoided felony charges and possible prison time*, WASH. POST (Jan. 25, 2016), https://www.washingtonpost.com/world/national-security/how-david-petraeus-avoided-felony-charges-and-possible-prison-time/2016/01/25/d77628dc-bfab-11e5-83d4-42e3bceea902_story.html?utm_term=.b20c98e20a43.

[85] *Id.*

[86] *See, e.g.*, Michael Schmidt & Matt Apuzzo, *David Petraeus Is Sentenced to Probation in Leak Investigation*, N.Y. TIMES (Apr. 23, 2015), https://www.nytimes.com/2015/04/24/us/david-petraeus-to-be-sentenced-in-leak-investigation.html.

[87] *See, e.g.*, The Times Editorial Board, *A double standard on government secrets for David Petraeus*, L.A. TIMES (Mar. 5, 2015, 6:30 AM), http://www.latimes.com/opinion/editorials/la-ed-0305-petraeus-20150305-story.html.

[88] *See, e.g.*, Trevor Timm, *Petraeus receives no jail time, while whistleblowers face decades in jail*, FREEDOM OF THE PRESS FOUND. (Apr. 23, 2015), https://freedom.press/news-advocacy/david-petraeus-receives-no-jail-time-for-leaking-while-whistleblowers-face-decades-in-jail/.

[89] *See* Matt Zapotosky, *Federal prosecutors urge 'severe' sentence for ex-CIA officer in leak case*, WASH. POST (Apr. 21, 2015), https://www.washingtonpost.com/local/crime/federal-prosecutors-urge-severe-

Although the district court did not appear to accept this argument when it imposed Sterling's sentence,[90] this incident, nonetheless, highlights the legitimacy and fairness concerns associated with disparate enforcement against leakers of varying seniority. To mitigate these concerns, prosecutors should generally refrain from affording high-ranking leakers any leniency that would not be given to more junior officials under the same circumstances.

E. Whether Prosecution Would Threaten to Disclose Additional Classified Information

Leak prosecutions, like other criminal cases that involve classified subject matter, present government lawyers with difficult choices that implicate U.S. national security. In particular, the decision to charge an individual for leaking secret information to the press must account for the possibility that prosecution could result in further disclosures of classified material that could damage national security.[91] This issue is relatively straightforward when the government knows it must present classified information in its case-in-chief, since in those circumstances the risk of additional disclosure is well understood and accepted at the outset.[92] More commonly, however, the government will not fully understand the risks of greater disclosure until the prosecution is already underway.

After his or her indictment, an accused leaker may invoke defense theories that require classified evidence entirely distinct from the information that has already been disclosed to the public. For instance, a mistaken identity defense to a leak prosecution, in which the defendant argues that other individuals within his or her

---

sentence-for-ex-cia-agent-in-leak-case/2015/04/21/4c8d1f5e-c001-4757-9b2a-50adf23b8d3c_story.html?utm_term=.cd2f672f83c4.

[90] *See* Transcript of Sentencing Hearing at 23-26, United States v. Sterling, No. 1:10cr485 (E.D. Va. 2015), https://www.documentcloud.org/documents/2106803-jeffrey-sterling-sentencing-hearing-transcript.html.

[91] *See* Timothy J. Shea, *CIPA Under Siege: The Use and Abuse of Classified Information in Criminal Trials*, 27 AM. CRIM. L. REV. 657, 658 (1990).

[92] *See, e.g.*, Radsan, *supra* note 35, at 481 (describing prosecution's conscious decision to use classified information in its case-in-chief).

organization were responsible for the leak,[93] could require disclosing the identities of covert intelligence officers who had access to the same classified information as the defendant. Alternatively, leak defendants may attempt to introduce secret evidence related to alleged government misconduct that purportedly exonerates them.[94] The prospect of such defenses creates a potential "graymail" dilemma for the government, in which the prosecutor might be forced to choose between allowing a leaker who harmed national security to escape punishment and pursuing a prosecution that would itself threaten U.S. security interests.[95]

The Classified Information Procedures Act (CIPA) is the government's principal tool to mitigate the problem of graymail, but it has significant limitations. CIPA does not alter evidentiary rules on admissibility or the government's general disclosure obligations to criminal defendants, and it does not prohibit the introduction of classified evidence at trial.[96] The statute instead provides procedures for the pretrial evaluation of potentially discoverable classified information in an effort to balance a defendant's right to present an effective defense with the government's right to make an informed decision about a prosecution's potential effect on national security.[97] To that end, CIPA requires a defendant to inform the government of the specific classified information that he or she intends to use at trial, and it provides for pretrial in camera review of that information's relevance and admissibility.[98]

If, after in camera review, the court determines that the information is admissible, the government can move to introduce an unclassified substitute, such as a statement admitting relevant facts or a redacted summary of the information.[99] The court can

---

[93] *See* Joel Todoroff, *Verisimilitude in National Security Cases*, 16 N.Y.U. J. LEGIS. & PUB. POL'Y 1223, 1247 (2013).
[94] *Cf.* Radsan, *supra* note 35, at 466.
[95] Shea, *supra* note 91, at 658.
[96] Ian MacDougall, *CIPA Creep: The Classified Information Procedures Act and its Drift into Civil National Security Litigation*, 45 COLUM. HUM. RTS. L. REV. 668, 679-81 (2014).
[97] Radsan, *supra* note 35, at 447.
[98] 18 U.S.C.A app. III §§ 5(a), 6(a), 6(c) (Westlaw 2017).
[99] *Id.* § 6(c).

then deny the government's motion if it determines that the substitute evidence does not provide the defendant with "substantially the same ability to make [his or her] defense as would disclosure of the specific classified information."[100] Given how infrequently this issue is litigated,[101] there is considerable uncertainty regarding what may qualify as an acceptable substitute.

At least one Court of Appeals, however, has affirmed a district court's rejection of the government's proffered substitute evidence in a prosecution involving classified subject matter.[102] And in a more recent leak case, *United States v. Rosen*, the district court held that the government's proposed procedures to shield sensitive information from public view during trial were not authorized under CIPA's "substitute" provisions.[103] The government subsequently moved to dismiss all charges against the defendants just one month before trial after several years of litigation.[104]

The prosecution's decision in *Rosen* reflects the fact that the government's interest in punishing a leaker of national security secrets must at times give way to the imperative of preventing additional damaging disclosures. Since this outcome depends in large part on the actions of defense counsel and judges over whom the government lacks influence, it is impossible for prosecutors to fully anticipate the risk of additional disclosures when making the initial decision to charge a leaker. Accordingly, prosecutors should be prepared to continually revisit this decision throughout the duration of a leak prosecution. In doing so, of course, they should consult with their counterparts in the national security bureaucracy who have an interest in protecting the information that is at risk.

---

[100] *Id.*

[101] *Cf.* ROBERT CARY ET AL., FEDERAL CRIMINAL DISCOVERY 377 (2011) (discussing small amount of authority regarding the necessary balancing test).

[102] *See* United States v. Fernandez, 913 F.2d 148, 157-58 (4th Cir. 1990) (holding that the district court did not abuse its discretion in concluding that the defendant, who was charged with lying about his involvement in CIA resupply operations, was entitled to present classified details about the scope of CIA participation in those operations to support his defense that it was "highly unlikely that he would misrepresent a matter of which the CIA was intimately aware").

[103] United States v. Rosen, 487 F. Supp. 2d 703, 710 (E.D. Va. 2007).

[104] Neil A. Lewis & David Johnston, *U.S. to Drop Spy Case Against Pro-Israel Lobbyists*, N.Y. TIMES (May 1, 2009), http://www.nytimes.com/2009/05/02/us/politics/02aipac.html.

Ultimately, the prosecutor may determine that additional disclosures of sensitive information at trial are inevitable and that such disclosures would cause greater harm to national security than allowing the leaker to avoid criminal punishment. In that event, the government's interests are best served by dismissing the prosecution and pursuing only administrative sanctions against the leaker.

IV. CONCLUSION

The framework proposed here does not address every issue that could be relevant to the decision to prosecute a leaker under the Espionage Act. Rather, it provides several boundaries that cabin the exercise of prosecutorial discretion in an effort to enhance the effectiveness and legitimacy of the government's approach to combating national security leaks. Within those boundaries, prosecutors should retain significant latitude to commence or decline prosecution in accordance with their limited enforcement resources and the duty to fairly and faithfully enforce federal criminal laws.[105]

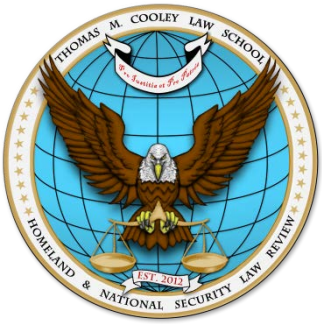
This framework also mitigates certain concerns voiced by critics of the Obama administration's approach to prosecuting leakers. Admittedly, the constraints imposed by this framework do not go as far as many reformers would hope. For instance, the constraints do not preclude the prosecution of individuals who are motivated to leak for altruistic reasons or require the government to establish that a putative defendant leaked information with the specific intent to harm U.S. national security.[106] However, the framework ensures that leak prosecutions are limited to government employees and contractors who are formally entrusted with classified information. It also instructs prosecutors to refrain from granting leniency to senior officials at the expense of lower-level employees. Most importantly, the proposed framework mitigates the issue of pervasive over-classification in leak prosecutions by requiring the prosecutor to establish that a leak caused actual harm to U.S. national security interests.

---

[105] *See* U.S. ATTORNEYS' MANUAL, *supra* note 11, at § 9-27.110.
[106] *See, e.g.*, Vladeck, *supra* note 3, at 232.

Many reform advocates would prefer that these policies be implemented through legislative action,[107] but it is unlikely that they can succeed on Capitol Hill. Despite the long-held view that the Espionage Act is severely flawed,[108] recent efforts to revise the Act have failed and the current political climate appears hostile to any liberalization of U.S. national security laws.[109] Thus, the most viable way to further these goals, at least on an interim basis, may be for the Executive Branch to adopt self-imposed reform measures in the form of official policy guidance clarifying its enforcement approach and limiting its discretion with respect to leak prosecutions. The Obama Administration took a positive step in this direction when it limited the ability of federal law enforcement officials to investigate the news media during leak investigations,[110] but its policy guidance to that effect did not explain the administration's broader approach to the prosecution of national security leakers.[111] The Trump Administration can and should go further by adopting the framework proposed here as official DOJ policy.

[107] *See, e.g.*, Mary-Rose Papandrea, *The Publication of National Security Information in the Digital Age*, 5 J. NAT'L SEC. L. & POL'Y 119, 128-29 (2011).
[108] *See, e.g.*, Edgar & Schmidt, *supra* note 16, at 930 (observing that the Espionage Act "implacably resist[s] the effort to understand").
[109] *See* ELSEA, *supra* note 26, at 27-30 (describing multiple historical failures of attempted legislative updates).
[110] *See* Att'y Gen. Memo, *supra* note 10.
[111] *Id.*


THOMAS M. COOLEY LAW SCHOOL
HOMELAND & NATIONAL SECURITY LAW REVIEW
EST. 2013