Just Short of Cyberwar: A Focus on *Jus Ad Vim* to Inform an Ethical Framework for Cyberspace

Al Lewis
American Military University

Abstract

Cyber conflict has yet to reach the lethality that defines war. As such, it has become the preferred method of engagement for nation-states. However, in its current state, there is no ethical framework to guide the policymaker. This article focuses on the concept of *jus ad vim* (just short of war) to inform an ethical framework for cyber conflict. This proposed framework is founded on five separate concepts pulled from the literature: intentional cyberharm, preventative force, punctuated deterrence, cyber sovereignty, and international response. Herein, two pivotal case studies, the Stuxnet worm against an Iranian nuclear facility and the Israeli Defense Force's (IDF) use of a kinetic strike in response to a cyberattack, are explored using a Grounded Theory approach. This article concludes that these concepts, as demonstrated through the case studies, can form the basis for ethical decision-making across cyberspace.

Keywords: *jus ad vim,* cyberwar, cyber sovereignty, political warfare, Just War Theory (JWT), cyberspace

Poco antes de la guerra cibernética: un enfoque en *Jus Ad Vim* para informar un marco ético para el ciberespacio

Resumen

El ciberconflicto aún tiene que alcanzar la letalidad que define la guerra. Como tal, se ha convertido en el método preferido de participación de los estados-nación. Sin embargo, en su estado actual, no existe un marco ético para guiar al hacedor de políticas. Este artículo se centra en el concepto de *jus ad vim* (justo antes de la guerra) para informar un marco ético para los conflictos cibernéticos. Este marco propuesto se basa en cinco conceptos separados extraídos de la literatura; daño cibernético intencional, fuerza preventiva, disuasión puntuada, soberanía cibernética y respuesta internacional. Aquí, dos

 doi: 10.18278/gsis.5.2.3

estudios de caso fundamentales; el gusano Stuxnet contra una instalación nuclear iraní y el uso de la Fuerza de Defensa de Israel (FDI) de un ataque cinético en respuesta a un ciberataque se exploran utilizando un enfoque de teoría fundamentada. Este artículo concluye que estos conceptos, como se demuestra a través de los estudios de caso, pueden formar la base para la toma de decisiones éticas en el ciberespacio.

Palabras clave: *jus ad vim*, guerra cibernética, soberanía cibernética, guerra política, teoría de la guerra justa (JWT), ciberespacio

差点成为网络战：运用*Jus Ad Vim*提出一个网络空间伦理框架

摘要

网络冲突尚未达到能定义为战争的杀伤力。照此，网络冲突已成为民族国家的优先接触措施。然而目前看来，还不存在能指导决策者的伦理框架。本文聚焦于*jus ad vim*（不及战争）概念，以期提出一个针对网络冲突的伦理框架。该框架基于从文献中提取的五个不同概念：蓄意网络伤害、预防措施、间断威慑（punctuated deterrence）、网络主权、以及国际响应。使用扎根理论方法探究了两个关键性案例研究：以伊朗核工厂为目标的震网蠕虫病毒，和以色列国防军（IDF）为回应网络攻击而发起的动能袭击。本文结论认为，案例研究所证明的概念能形成网络空间的伦理决策基础。

关键词：*jus ad vim*，网络战，网络主权，政治战，正义战争理论（JWT），网络空间

Introduction

The ethical considerations for both deciding to enter a war (*jus ad bellum*) and the conduct once embattled in war (*jus in bello*) are well established. These ethical tenants comprise the underpinnings of the Just War Theory (JWT). While vital relative to war, much of today's conflict, specifically cyber conflict, falls just short of war (*jus ad vim*). The study of *jus ad vim* is not well established, nor does an ethical framework exist to guide actions before or during these conflicts. This article focuses on the concept of *jus ad*

vim (just short of war) to inform an ethical framework for cyber conflict. This proposed framework is founded on five separate concepts pulled from the literature: intentional cyberharm, preventative force, punctuated deterrence, cyber sovereignty, and international response. When considered collectively, these concepts form a framework to aid in ethical decision-making.

In what follows, the first section provides a background discussion on war and the impact technology has had in its transformation. Specifically, the transition from conventional war and JWT to cyberspace and *jus ad vim* is addressed. This section is followed by an analysis of the ethics of war and conflict where gaps in current literature and understanding are made apparent. The third section addresses the application of Grounded Theory across two pivotal case studies: the Stuxnet worm and the Israeli Defense Force (IDF) kinetic strike in response to a cyberattack. These two studies serve as forerunners in the advancement of cyber conflict. As such, these case studies provide fertile ground to build an ethical framework for the application of *jus ad vim* in cyberspace. The article concludes with an analysis of the state of cyber conflict and advocates for the establishment of an ethical framework across the entire spectrum of *jus ad vim* within cyberspace.

Background

The impact of technology on warfare is comparable to the evolution of information collection. Hammes (2004) chronicles the generations of warfare and in doing so lays out the role of technology in the advancing of military tactics. For example, maneuverability is the defining characteristic of the third generation of warfare (Hammes 2004, 13). The technological advances of "reliable tanks, mobile artillery, motorized infantry, effective close air support, and radio communications" surpassed the trench warfare of World War I, thus creating the conditions for a highly maneuverable fighting force (Hammes 2004, 13). Similarly, the creation of information technologies has created the modern ecosystem referred to as cyberspace. The speed, ubiquity, and anonymity of these technologies have fundamentally changed the tactics of information collection and the strategies that guide them. As such, it is essential to examine how war and cyber conflict intersect.

The last time the United States declared war was in World War II; not even the fight against global terrorism, dubbed the "war on terrorism," reaches the high-water mark of an official declaration of war (Bradley and Goldsmith 2005, 2048; Schwartau 1998). Correspondingly, the US has "diplomatically and politically avoided the term [war] in the interests of 'peace'" (Schwartau 1998, 55). Notably, no war has resulted from cyber actions. Indeed, to date, "no one has ever been killed by a cyber capability" (Perkovich and Levite 2017, 4). Perhaps it is the promise of cyber lethality that has generated the concept of cyberwar, as lethality is war's defining feature (Dipert 2010, 386). Some researchers see the potential severity of

cyberattacks as satisfying the *casus belli* (just cause) for going to war; this also aligns with the equivalence principle, wherein a significant cyberattack could justify a military response (Dipert 2010, 405; Kello 2017, 196).

In its current state, cyberwar is more indicative of a politically motivated cyber struggle, where attribution is tenuous, and maintaining intellectual property and state secrets are the measures of success, not a body count. The reality of today's cyber engagements appears to be more aligned to the concept of political warfare through the cyber domain, than to a cyberwar. "In the broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives" (Blank 2017, 82). There is no doubt that the United States is engaged in "intense cyberconflict" with other nation-states; however, none of these conflicts has risen to the level of war (Singer and Friedman 2014, 121). That means that all actions in cyberspace, up until now, have been short of war. The ability for one nation to impose its will on another, absent a war, is political nirvana.

There is no expectation that technology will plateau, and states will enter a form of cyber-stasis. As stated in the National Cyber Strategy: "America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected information technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed, and new threats continue to emerge" (National Cyber Strategy 2018, 1).

Similarly, the US military recognizes five military battlespaces – land, sea, air, space, and cyberspace. As the world has grown in complexity and connectivity, traditional concepts that have defined military objectives, such as terrain and borders, have become increasingly blurred and ambiguous. "There are no longer battlespaces that operate independently, or more to the point, independent of cyberspace; as cyberspace is the battlefield from which all battlefields are amplified" (Lewis 2019). The Department of Defense (DoD) considers cyberspace to be "a part of the so-called *information environment*, defined as the 'aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (Porche, Sollinger, and McKay 2011, 19). To this end, the information environment includes both government and commercial entities, bringing to bear vast capabilities across the entire spectrum of information operations (IO) (Armistead 2004; DoD 2018).

Significantly, cyberspace functions as operational continuum, where cyber conflict is a constant. War, on the other hand, is distinctly defined through time. This dichotomy gives rise to the urgency in need for ethical guidelines within cyberspace. It is in this context that the application of *jus ad vim* (just short of war) can aid in un-

derstanding how current ethical frameworks focused on JWT are inadequate for the weaponization of cyberspace. As Michael Walzer (2015, 85) argues, "it is obvious, for example, that measures short of war are preferable to war itself whenever they hold out hope of similar or nearly similar effectiveness." *Jus ad vim* has found advocacy in policing actions and military measures short of war (MMSoW), with emphasis on use-of-force and less-than-lethal methods (Brunstetter and Braun 2013; Ford 2013; Kaplan 2019). In its current state, cyberwar does not exist in the context of JWT.

The extent of the relationship between cyberspace and war is unclear. On the one hand, cyberspace provides a conduit for war. On the other hand, it may become the manifestation of war itself. What is clear, however, is that cyberspace will play a pivotal role in all future actions in furtherance and defense of national objectives. Correspondingly, there is a need for moral clarity in cyberspace; by applying *jus ad vim* (just short of war) to cyberspace, this research aims to take a step forward in providing such clarity.

Review of the Literature

A literature review was conducted to determine the current state of *jus ad vim.* There is a scarcity of academic writing on *jus ad vim* and specifically its application to cyberspace. As such, every attempt was made to utilize primary sources from peer-reviewed academic journals, conference proceedings, and technical reports from cybersecurity researchers. However, secondary sources were included when no primary sources were available. Secondary sources included news articles, security blogs, and books in determining the current state ethics as they pertain to *jus ad vim* in cyberspace.

Two themes dominated the review. The first reveals that the principles that comprise JWT are the de facto standard by which the ethical nature of conflict is measured. Second, the idea of *jus ad vim* and its applicability outside the framework of JWT is under contention. As such, the argument for an ethical framework operating outside of war, hence outside the principles of JWT, is not unanimous. To date, the application of *jus ad vim* can be observed primarily in use of force models within law enforcement and MMSoW, neither of which address cyberspace, nor put forth an ethical framework.

It is nearly impossible to analyze the ethics of war, or actions *just short of war,* outside of the framework of JWT. JWT reflects the works of the great philosophers Augustine (345–430) and Thomas Aquinas (1225–1274) (Dorbolo 2001; Orend 1999, 324). The two major sections of JWT are *jus ad bellum* and *jus in bello* (Brunstetter 2016: Dorbolo 2001; Frowe 2016; Macnish 2016, 96; Orend 1999, 344–45; Walzer 2015). *Jus ad belllum* is concerned with the justness of fighting a war, whereas *jus in bello* is concerned with the actions once the war commences (Orend 1999, 344–45). Walzer's (2015) seminal work frames the importance of mor-

al clarity in war. He asserts that JWT is about war and "moral philosophy" (2015, 335). As such, Walzer is a strong advocate for JWT.

That said, Walzer acknowledges that a space just short of war must exist; he refers to this as *jus ad vim.* He uses this concept to explain a state's assertion of power that does not meet the criteria of war (Ford 2013, 64). "The analytical starting point of *jus ad vim* is identifying certain categories of violence as falling short of war, and thus not governed by these special privileges" (Brunstetter 2016, 133). The concept of *jus ad vim* is appealing, as the manner, if not nature, of war, has evolved. Several theorists, Walzer among them, attempt to apply *jus ad vim* to new technologies and methods of employment to highlight its usefulness: specifically, the use of drones (Brunstetter 2016, 132; Ford 2013, 68; Frowe 2016, 119; Galliott 2016, 174; Kaplan 2019).

Some scholars debate the need for*jus ad vim* (Brunstetter 2016; Ford 2013; Frowe 2016). Helen Frowe and C.A.J. Coady contend that *jus ad vim* is not a panacea, nor is it entirely well established (Ford 2013; Frowe 2016). The limited implementation of *jus ad vim* is not surprising, as the nature of conflict, its conduct, by whom, and from where have become fluid. Walzer's initial examination of *jus ad vim* was itself limiting, as his vision for application applied strictly to "collective security" (Ford 2013, 65).

Frowe contends that those advocating for *jus ad vim* lack the requisite depth of understanding of JWT. Whereas others, such as Brunstetter (2016) and Ford (2013), contend that JWT is inadequate for areas outside conventional warfare. Conversely, Frowe believes advocates of *jus ad vim* place "unwarranted weight on whether something counts as war" (Frowe 2016, 122). Arguably, the literature is unsure if actions in cyberspace constitute an act of war or whether JWT is the correct ethical framework (Barrett 2017; Beard 2016; Dipert 2010; Kuru 2017). The majority of the literature agrees that operations in cyberspace can constitute a use of force (Barrett, 2017; Dipert 2013; Foltz 2012, 40; Kuru 2017; Schmitt 2013; Stockburger 2016), with Wortham being a rare exception only in that she differentiates cyberattacks from cyber exploitation (2012, 645).

Lastly, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* represents the acknowledgment that international laws are noticeably absent within the realm of cyberspace and that clarity surrounding the definitions, laws, and ethical frameworks needed to advance modern society is needed (Barrett, 2017; Foltz 2012; Rota 2018; Schmitt 2013). The strength of cyberspace lies within its resiliency. Conversely, the resilience obtained through a fault-tolerant persistence also makes attribution and signal detection questionable, meaning that the cyberspace milieu casts doubt on the degree of guilt and culpability of action. As such, the lack of international law is problematic, as the tactic of mirroring traditional policy, such as the all or nothing policy of deterrence, is not a realistic solution for cyberspace (Kello 2017, 197).

Despite the contretemps among scholars seeking to understand and define the ethical boundaries for modern conflict, *jus ad vim* holds the promise of adding clarity to the debate (Kaplan 2019). In doing so, it may well provide policymakers with an iterative framework from which to base their ethical decisions as they grapple with the nuance of cyber conflict.

Methods

This research explores the utility of *jus ad vim* as it applies to cyber conflict, by examining two cyber firsts: the Stuxnet cyberattack against Iranian nuclear centrifuges and the IDF's kinetic airstrike in response to a Hamas cyberattack. These attacks serve as milestones in cyber conflict and highlight the inevitable conflation of the physical and virtual realities of modern society. Further, the rapidity of technological and political change demands urgency in defining the ethical and legal issues facing policymakers. As such, each case study is examined via five principles: intentional cyberharm, preventative force, punctuated deterrence, cyber sovereignty, and international response.

Intentional cyberharm provides for the expansion of cyber acts and actors to include both cybercrime and civilians. The idea of intentional cyberharm is not constrained by physical damage, although Stuxnet certainly achieved that; instead, it is broad enough to cover the majority of harm conducted by cyber means, such as state-sponsored cybercrime and IO. Intentional cyberharm is significant in cyberspace, as cyberspace encompasses entire populations, not just state actors. As such, intentional cyberharm can accommodate the individual actor and nation-state actions. The intentionality of harm can be problematic in cyberspace. For example, many standard network tools can serve a dual purpose from which nefarious acts can be committed intentionally or not. That said, malicious software contains the intent of its author in its code and subsequent execution.

Preventative force provides for a moral obligation to act in preventing escalation. Preventative force, as Arquilla writes, "is a strategic construct designed for using a modicum of violence to thwart the rise of a fresh danger, to keep an ongoing conflict from widening, or perhaps most important, to avoid the outbreak of a large-scale conflict" (2017, 99–100). In the case of cyberspace, a preventative force need not necessarily rise to the level of violence, but may reside in assertive action. "The Tallinn Manual group of experts agree the 2009 Stuxnet cyberattack against Iran's nuclear facilities constituted 'use of force,' but they are divided on whether it constituted an 'armed attack'" (Oxford Analytica 2019).

Punctuated deterrence is "an approach that accepts the possibly insurmountable limitations of denial while rejecting the policymakers' pervasive obsession with absolute prevention. Instead, it calls for more flexible logic of punishment that addresses not single actions and particular effects, but *series* of actions and *cumulative* effects" (Kello

217, 197). No defense is impenetrable. In cyberspace, the advantage favors offensive operations. By accepting a level of adversarial success, the defense becomes free to allocate limited resources to the most critical areas, rather than the strategy of attempting to protect everything, all the time, from everyone. Punctuated deterrence changes the economics for the attacker. As such, punctuated deterrence enables the policymaker to prioritize resources for self-defense.

Cyber sovereignty defines boundaries, providing clarity on spheres of influence and defense. The preservation of sovereignty is inextricably linked to war. Michael Walzer (2015, 51–52) mentions both territorial integrity and political sovereignty as the borders by which states define themselves and, consequently, actions against them. Historically, sovereignty is about control. Specifically, "supreme authority within a territory" (Philpott 2016). Although "as the world has grown increasingly entangled, traditional concepts that have defined military objectives, such as terrain and borders, have become increasingly blurred and ambiguous" (Lewis 2019). It comes as no surprise then that states are seeking to expand their influence and the idea of sovereignty across cyberspace.

As physical resources aid in establishing the power of the state, so too in cyberspace. Advanced states, given their resources, have more influence; this extends to cyberspace, wherein states are increasingly becoming cyber-centric, thus transforming into cyber-states. A cyber-state is defined herein as a nation-state, dependent on cyberspace, wherein the entirety of the state, including its government, citizenry, and infrastructure, seamlessly integrates technology across its society for the advancement of its national defense and political goals.

Authoritarian regimes such as China and Russia have made significant moves toward controlling the content of internet traffic into and out of their respective countries. Also, by leveraging a series of legal and technical measures to ensure that their versions of cyber sovereignty reflect "the stance that cyberspace should be defined and ruled by state boundaries" (Iasiello 2017, 1). In this vein, China and Russia could be viewed as early adopters of the notion of "Cyber Westphalia," wherein it is predicted that "most states will delineate borders in some measure across the formerly ungoverned, even chaotic cyberspace substrate" (Demchak and Dombrowski 2013, 36).

As states attempt to solidify what cyber sovereignty could mean to them, a part of that equation will likely include the legality and morality of actions in the event of a cyberattack. For instance, can a cyberattack constitute a breach of sovereignty? In its current state, cyberattacks have not reached the level of cyberwar, meaning that states do not see them as a threat to their sovereignty. The lack of concern is likely to change if cyber sovereignty is established and internationally accepted.

The international response serves as a "pseudo court" for accept-

ability of action. Correspondingly, lawyers are trained in analogical reasoning. Meaning, as new events occur, lawyers look to the past to identify precedent to apply to the new situation (Texas A&M School of Law Media 2015, 01:43). Additionally, international lawyers observe state responses to acts of aggression as a barometer for the legal and political threshold (Fidler 2011). In other words, how states respond sets the tone for international norms. States may demonstrate a controlled response if they calculate the cost of an attack too high. This is "what some thinkers call 'self-deterrence,' whereby the attacker decides not to attack because he believes that the negative consequences will affect him as well" (Kello 2017, 201). In the end, international response to conflict serves as a basis for judging the morality of action.

The research contained herein is confined to the moral guidance offered by *jus ad vim* to "uses of state power short-of-war" (Ford 2013, 65). However, cyberspace consists of far more participants than those responsible for state actions; therefore, the principles of *jus ad vim* should not be restricted to state actors.

Grounded Theory enables the development of a theory by discovering patterns in data (Scott 2009). The method contained herein leverages the Paradigm Model of Grounded Theory, where causal conditions of a phenomenon are represented by technological change and the avoidance of war declarations (Miller and Fredericks 1999, 538). The phenomenon examined are two case studies representing significant shifts both in context and the intervening conditions, wherein one represents a clandestine operation and the other an implementation of overt force.

Moreover, the strategies and actions that result have demonstrated the consequences of cyber conflict as a means in furtherance of state goals without an ethical framework. As the variables of an ethical framework for actions just short of war are yet undefined; the commonalities and differences between conventional war, as depicted in JWT and the dynamic nature of cyberspace viewed through *jus ad vim,* will aid in developing variables for future research.

Case Study: Stuxnet

Iran's 2006 response to unsuccessful negotiations with the United States and European leaders was to resume its uranium enrichment program at the Natanz facility (DeIviscio et al. 2017; Langer 2013, 7–8). By 2008, engineers at the Natanz facility were experiencing a variety of malfunctions and breakages in their centrifuges (DeIviscio et al. 2017; Gates 2012). The engineers experienced "low morale," as the seemingly inexplicable malfunctions appeared beyond their reasoning (Singer and Friedman 2014, 117). The possibility of being the victim of a cyberattack was never considered, for two excellent reasons. First, the systems in the Natanz facility were air-gapped and, therefore thought to be impenetrable to cyberattack. Second, no cyberattack had ever been capable of physical damage, and the

centrifuges were experiencing physical damage (Singer and Friedman 2014, 117).

Discovered in 2010, Stuxnet is the name given to the most advanced computer worm ever created. A computer worm is a self-replicating software program designed to traverse from computer to computer across a network. In the case of Stuxnet, the worm contained four zero-day exploits. A zero-day is an unknown software vulnerability, making them both rare and valuable. Furthermore, the worm was highly specific in its targeting, targeting only "a specific type of program used in Siemen's WinCC/PCS 7 SCADA control software" (Singer and Friedman 2014, 116). The control systems referred to as SCADA are defined as "an acronym for Supervisory Control And Data Acquisition, a category of computer programs used to display and analyze process conditions" (Langer 2013, 9). Additionally, the industrial controllers targeted were only those that were configured as a "cascade of centrifuges of a certain size and number (984) linked together ... the exact setup at the Natanz nuclear facility" (2014, 116).

In the absence of official acknowledgment, Stuxnet remains an enigma. "To date, no country or group has claimed responsibility for developing what has been termed by some as 'the world's first precision guided cybermunition'" (Kerr, Rollins, and Theohary 2010, 2). However, the resources and skills required to create and successfully infiltrate Stuxnet into its intended target indicate nation-state sponsorship. Initial analysis indicated that "countries thought to have the expertise and motivation of developing the Stuxnet worm include the United States, Israel, United Kingdom, Russia, China, and France" (2010, 2). Later, it was leaked to "have been a collaborative effort between US and Israeli intelligence agencies, known as 'Olympic Games'" (Singer and Friedman 2014, 117–18).

The mission of Stuxnet is believed to be to penetrate the Natanz uranium enrichment facility in Iran and create the conditions to cause the centrifuges to fail (Gates 2012; Kerr, Rollins, and Theohary 2010; Langer 2013, 11; Singer and Friedman 2014, 116; Zetter 2014). The ability to infect air-gapped systems is so difficult that designing air-gapped systems remains a cybersecurity best practice. Nevertheless, the creators of Stuxnet were able to penetrate the air-gapped systems within the Natanz facility, thus introducing the worm into a controller computer (DeIviscio et al. 2017; Fidler 2011, 57; Foltz 2012, 44; Gates 2012; Kerr, Rollins, and Theohary 2010, 4; Kushner 2013, 50; Zetter 2014).

Purportedly, the Olympic Games operation set the Iranian nuclear capabilities back by "a year and a half or two years" (DeIvscio et al., 2017, n.p.). The first known instance of a cyberattack to cause physical damage in the real world, Stuxnet has been referred to as "history's first field experiment in cyber-physical weapon technology" (Langer 2013, 3). Nevertheless, there was no cry of war, no suitable counterstrike, only a feeble attempt to

downplay its effectiveness by the Iranian regime (Fidler 2011, n.p.). Stuxnet remains an enigma as it broke all convention crossing the cyber and physical barrier while seeming warlike and peacekeeping at the same time.

Analysis

Cyberspace (Porche, Sollinger, and McKay 2011, 19) and cyberwar are portmanteaux, blending the words cyber and space/war. That said, however eloquently the terms blend, the concepts remain apart. Cyberwar, as defined herein, does not exist. A great failing of the *Tallinn Manual on the International Law to Cyber Warfare* is that the group of experts reinforces the notion that JWT applies to cyber operations (Schmitt 2015, v). Strictly speaking, current cyber operations are a step removed from the lethality that defines war (Dipert 2010, 398). The current operating environment, from a nation-state perspective, is that of a political war. As others have noted, "Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives" (Blank 2017, 82). That is not to say that cyberwar cannot exist, as the confluence of technology and war will continue to mature to the point where a war without cyberwar will become unthinkable. It appears inevitable that the ultimate maturation of any technology for the masses is its application within war. These dual-use technologies are the bedrock of modern warfare, with nuclear technology as its shining example.

An attack on a sovereign state's nuclear facilities is undoubtedly an act of war; however, a cyberattack is a different matter. Stuxnet was a cyberattack aimed at the heart of the Iranian nuclear program. The cyberattack caused physical damage to the centrifuges and unequivocally hampered Iranian state ambitions. Remarkably, Stuxnet did not cause a cyberwar, nor did it cause a conventional one. As such, the ethical considerations and subsequent moral framework fall outside JWT. It is imperative to examine Stuxnet through the prism of *jus ad vim* rather than of JWT, since cyberwar is noticeably absent.

Intentional Cyberharm

The duality of cyber-based technologies reflects the need for additional considerations outside the JWT. Randall Dipert (2010, 397) introduces the concept of intentional cyberharm (intentional cyberattacks) as a term sufficiently broad for cyber-ethics. A cyberattack can have sweeping implications. For example, "The emergence of the Stuxnet worm is the type of risk that threatens to cause harm to many activities deemed critical to the basic functioning of modern society" (Kerr, Rollins, and Theohary 2010). As such, Stuxnet appears to be a textbook example of Dipert's concept of intentional cyberharm. That is to say, one or more "political organizations or their military services" intentionally caused harm, via the cyber domain, to another "political organization or their military services"

(Dipert 201, 398). The Stuxnet code was crafted in a manner that was highly specific in identifying and harming targeted infrastructure.

Preventative Force

Significantly, Stuxnet was crafted in such a way that it only harmed its intended target, had built-in controls to become inert, and contained a self-destruct mechanism with an expiration date (Singer and Friedman 2014, 116, 119). Stuxnet embodies the concept of preventative force, as made apparent in delaying the Iranian nuclear program. Whether or not this was the intention can be debated; however, by using an effects-based approach, as favored in the Tallinn Manual, Stuxnet was remarkably successful in the application of a preventative force (Kuru 2017, 52).

As Ford asserts, "Walzer argues that while preventative war is normally not justifiable, under certain specific conditions, we might be able to justify preventative force" (2013, 66). Walzer underestimates the application of preventative force in cyberspace, as it is arguably a current best practice from a nation-state perspective. Put another way, nation-states not engaging in preventative force are substantially diminishing their ability to impose their will within cyberspace. In this context, Stuxnet was designed to fulfill a preventative in stalling nuclear escalation.

Punctuated Deterrence

Stuxnet serves as a modern example of cyber diplomacy. As negotiations surrounding Iran's nuclear program faltered, Iran countered with a renewed emphasis on its uranium enrichment program. In the context of punctuated deterrence, the creators of Stuxnet recognized the inevitability of Iran continuing its nuclear program; therefore, they sought to change the economics by not only inhibiting its acceleration but through the demonstration of a capability far beyond that of the rest of the world's cyber-powers, let alone Iran's. The message was clear, the continuation of the program, without negotiations, will be countered, possibly with previously unknown capabilities.

Cyber Sovereignty

Did Stuxnet infringe on the cyber sovereignty of Iran? In its current state, cyber sovereignty is more of an idea than a reality. Furthermore, Iran arguably lays no claim to cyber sovereignty as they lack the maturation of cyber defense. In this vein, Iran was not capable of launching any counterattack, cyber or kinetic, as no attribution was evident, and war remains a disfavored option. Sovereignty, cyber or otherwise, cannot be asserted if it cannot be defined and protected.

International Response

Self-deterrence was a significant factor in the international reaction to Stuxnet. Stuxnet was the shot heard around cyberspace. It broke from theory and demonstrated something the world had never seen. Only an unwise adversary would not question what more the creators could be capable of in light of this demonstration. The natural paucity of

action stemming from the awe-inspiring technological leap may explain the deafening silence from international lawyers and policymakers. This is likely one of the reasons that it did not escalate to a war—that and the fact that Iran could not engage in a cyberwar, and conventional war was also unlikely with the creators of Stuxnet, as they did not appear to have any intention of going to war, only preventing one, a nuclear one at that.

Comparatively, as Arqullia (2017) points out, "Iranian and international reactions were likely far more muted than would have been the case in the wake of an air raid, a missile strike, or a commando attack" (108). Significantly, according to NATO, cyber operations fail to achieve a level of violence that equates them to military operations; as such, NATO is reluctant to respond (Blank 2017, 83). For Stuxnet, this rings especially true, as no lives were lost, and only the intended targets were impacted, leaving no collateral damage. It would be difficult for any state to obtain international support for an escalation to war for what amounted to some broken parts.

Case Study: Israeli Defense Force's (IDF) Kinetic Response to Cyber Operations

The Islamic Resistance (Hamas) seized control of the Gaza Strip in 2007. Since that time, there have been a series of conflicts with Israel (Central Intelligence Agency 2019). Beginning in 2012, Hamas has conducted a series of increasingly sophisticated cyberattacks against Israel (Dostri 2018). The attacks progressed from attacks on websites to Distributed Denial of Service attacks to social engineering to implanting spyware on mobile phones (Dostri 2018). Starting in May 2018, the Palestinians "have stepped up protests that sometimes featured incendiary balloons sent into Israel and improvised explosive devices and grenades. Israel has responded with deadly fire it said was necessary to protect its border. The two sides have inched closer to their fourth war in the past decade, with every truce interrupted by new spasms of violence" (Schwartz and Lieber 2019, n.p.).

Consistent with its tragic history, fighting broke out during the first weekend of May 2019 between Hamas and the IDF. The fighting was the typical exchange of Hamas rockets and mortar shells with Israeli airstrikes in response (Cropsey 2019; Gross 2019; O'Flaherty 2019). However, the intensity of the exchange was atypical. As reported, "The fighting raged all weekend. Over 600 rockets were fired toward Israel from the Gaza Strip, while Israeli forces conducted strikes on what it said were more than 250 military targets in the Palestinian enclave" (Schwartz and Lieber 2019, n.p.). Nevertheless, the volume and intensity of the munitions exchange were not the defining moment of the conflict. That distinction came in the form of an Israeli response to a Hamas-launched cyberattack during the kinetic engagement.

The cyberattack launched on May 4, 2019 by Hamas was claimed to be aimed at "harming the quality of

life of Israeli citizens" (Cropsey 2019, n.p.). In response to the cyberattack, which IDF claims to have thwarted, was to counter with an immediate airstrike, destroying the building containing Hamas's cyber operations (Gross 2019). "Israel's response marks the first time that a country has used immediate military force to destroy a foe's cyber capability in an active conflict" (Cropey 2019; Liptak 2019).

The cyberattack by Hamas highlights their evolution. Israel had been carefully monitoring Hamas's foray into cyberspace and witnessed their slow increase of capabilities (Shahaf 2018). Slow in cyberspace is a relative concept, as technology growth and exchanges can quickly fill a capability void. To this end, Israel had been a victim of previous Hamas cyberattacks, illustrating that they have grown "bolder in the tactics" (Dostri 2018, n.p.). It is likely that Hamas's increasing cyber capabilities were aided by its supporters. "Hamas, probably with Iranian assistance, established a headquarters to conduct cyber operations. This is probably why Israel responded decisively in both the cyber domain and in the physical world" (Cropey 2019, n.p.). That said, the intensification of cyber-based capabilities within a terrorist organization presents another level of malevolence, thus exhibiting a clear and present danger.

Analysis

The inclusion of the kinetic strike in response to a cyberattack appears outside of *jus ad vim*; however, it is not. In this case, Israel and Hamas are not at war, and the effects of the counterstrike did not cause war. This cyber-first is included to highlight the increasing pervasiveness of cyberspace, as terrorist organizations such as Hamas have moved beyond online recruitment into cyber operations. The entrance of terrorist organizations, such as Hamas, into cyber-based operations, signifies an inevitable increase in intentional cyberharm.

Intentional Cyberharm

Hamas intended to increase the level of harm on the streets of Israel when it conducted a cyberattack against Israel during a conventional kinetic engagement (Cropsey 2019; Gross 2019; O'Flaherty 2019). Israel's immediate kinetic response to the cyberattack indicates that this scenario was considered and decided in their military planning prior to the engagement (Cropsey 2019). What is unknown is the Israeli requirements for such a forceful response. Presumably, as depicted in the Tallinn Manual, "its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (Schmitt 2013, 22). What is clear is that the Israeli leadership felt its populace sufficiently threatened and thereby it felt justified in its response.

Preventative Force

Not all cyberattacks are created equal, nor do they all elicit the same response. It may be, as Finley (2016) suggests, "only some types of cyber-attack are equivalent to armed, kinetic attack, and give prima facie warrant for armed, kinetic defence" (358). In the case of

the Israeli response, since the cyberattack was not successful, it is unclear if the attempt and the intent are ethically equal to the effects in deciding to conduct a kinetic counterattack. It may well be that the position was that of deterrence through a preventative force model, wherein Hamas had achieved a level of cyber capability that was no longer deemed an acceptable risk to the State of Israel. In this light, destroying Hamas's cyber capability presumably saved Israeli lives in the long run.

Punctuated Deterrence

The Israeli stance toward Hamas's offensive cyber capability can be considered through the concept of punctuated deterrence. The series of concerted efforts on the part of Hamas to penetrate the IDF and Israeli leadership are prime conditions for punctuated deterrence, as the series of actions on the part of Hamas warrant an appropriate reaction from Israel. In the case of the kinetic response, it is evident that Hamas had crossed the Israeli threshold for implementation of a deterrent.

The choice of a kinetic response sends a strong message, as Israel is an elite cyber-state, or as Prime Minister Benjamin Netanyahu contends, Israel is "a global cyber security power" (Globes 2016, n.p.). As such, a cyber response is always an option for any form of aggression. The decision to destroy a capability rather than thwart its effect is significant and cannot be taken out of the context of the prolonged engagement history of the parties involved. The decision to destroy Hamas's cyber operations could be as simple as Israel not wanting to engage the terrorist organization on two fronts simultaneously (cyber and physical). The exact reasons for the employment of a kinetic response are not known; however, the cost for a cyberattack aimed at harming Israeli citizens has significantly increased.

Cyber Sovereignty

By comparison, Israel is in a far better position to assert the concept of cyber sovereignty as they are one of the most capable cyber-states in the world (Globes 2016). As such, Israel possesses the ability to defend and extend its cyber reach. Effectively, from a cyber perspective, it is the supreme authority within the territory. Hamas, on the other hand, can make no such claim (Shahaf 2018). Despite their increasing cyber capabilities, they lack the defensive capability and offensive skill and capacity to rule over a cyber dominion. Further, Hamas was the aggressor in cyberspace, as such, they would have had to breach Israeli networks. A breach of Israeli networks could be viewed as a breach of its cyber sovereignty.

International Response

The first real-time kinetic counterstrike to a cyberattack received a response similar to that of Stuxnet: hardly a ripple. In international terms, no response is interpreted as a form of acquiescence. The implications are far-reaching in that the stakes for engaging in cyberspace, which can hardly be avoided, have increased significantly. The argument can

be made that the international community is against a nuclearized Iran and the increasing capabilities of the terrorist organization Hamas (Department of State 2017). From this perspective, both the cyberattack that unleashed a new cyber weapon in Stuxnet and the immediate kinetic strike in response to a terrorist-based cyberattack have given pause to the international community as it struggles to determine the ethical boundaries in cyberspace.

Conclusion and Discussion

The nature of conflict has changed. Cyberspace provides greater reach, anonymity, and influence whereby states can assert their agendas. "While states have always used sublethal harms to weaken adversaries economically, militarily, ideologically, culturally, and politically, technological developments have magnified the regularity and effectiveness of these practices, particularly against free societies" (Barrett 2017, 467). These two cyber firsts, Stuxnet and the IDF's kinetic response to a cyberattack, are pivotal moments that changed the nature of cyber conflict and set the precedent for future conflict. The lack of international response has permitted its increased use as a method of political warfare.

For example, Reuters recently reported that the US carried out a "secret cyber strike on Iran" in response to the Iranian attack on Saudi Arabia's oil facilities on September 14, 2019 (Ali and Stewart 2019, n.p.). Ali and Stewart (2019) claim that it is a way for the US to counter Iranian aggression without escalating into a war: *jus ad vim* par excellence. As in the case studies discussed herein, the effectiveness is made apparent in the absence of war.

There is no expectation that technology will plateau or that states will enter a form of cyber-stasis. Policymakers acknowledge as much; therefore, it is necessary to look for signs of the type of change that will shift from the current state of *jus ad vim* into a cyberwar. As former President Obama is credited with stating: "The USA, for instance, has adopted the principle that retaliation against cyber-attacks may take the form not only of cyber-counter-attack but also attack by conventional military means" (Finley 2016, 358). Indeed, a kinetic response to a cyberattack may be the best indication of increasing dependence on cyberspace; thus, its debilitation may elicit such a response, rapidly creating the conditions for cyberwar.

The ethical framework defined in this article provides the phronesis for the application of *jus ad vim* in cyberspace. How states continue to pursue their interests in and through cyberspace has global ramifications for security and privacy. Furthermore, actions in cyberspace will remain under the watchful eye of the international community, as it continues to struggle with determining normal within the inchoate framework of international cyber law.

This article leverages the concepts of intentional cyberharm, preventative force, punctuated deterrence, cyber sovereignty, and international response as they apply to *jus ad vim*

in cyberspace. These concepts, viewed through the Stuxnet worm and the Israeli airstrike in response to a cyberattack, set the stage for the development of an ethical framework for cyberspace. The importance of this research lies in aiding the development of ethical considerations for cyberspace and providing moral clarity for the policymaker. Additional future research opportunities abound surrounding the triumvirate of cyberspace, ethics, and the law.

References

Ali, Idrees, and Stewart, Phil. 2019. "Exclusive: U.S. Carried out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack." *Reuters*. https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK.

Arquilla, John. 2017. "An Ounce of (Virtual) Prevention?" In *Understanding Cyber Conflict: 14 Analogies.* Chapter 6, 99–110. Washington, DC: Georgetown University Press.

Barrett, Edward. 2017. "On the Relationship Between the Ethics and the Law of War: Cyber Operations and Sublethal Harm." *Ethics & International Affairs 31*(4): 467–77.

Beckerman, Gal. 2006. "Reuters Takes a Hit in the War on the MSM." *Columbia Journalism Review.* https://archives.cjr.org/behind_the_news/reuters_takes_a_hit_in_the_war.php.

Blank, Stephen. 2017. "Cyber War and Information War à la Russe." *Understanding Cyber Conflict: 14 Analogies.* Chapter 5, 81–98. Washington, DC: Georgetown University Press.

Bradley, Curtis A., and Jack L. Goldsmith. 2005. "Congressional Authorization and the War on Terrorism." *Harvard Law Review, 118* (7*)*. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5902&context=faculty_scholarship.

Braun, Megan, and Daniel Brunstetter. 2013. "Rethinking the Criterion for Assessing CIA-Targeted Killings: Drones, Proportionality and Jus Ad Vim." *Journal of Military Ethics 12*(4): 304–24.

Brunstetter, Daniel. 2016. "Jus Ad Vim: A Rejoinder to Helen Frowe." *Ethics & International Affairs 30*(1): 131–36.

Brunstetter, Daniel, and Megan Braun. 2013. "From Jus Ad Bellum to Jus Ad Vim: Recalibrating Our Understanding of the Moral Use of Force." *Ethics & International Affairs 27*(1): 87–106.

Central Intelligence Agency. 2019. "Gaza Strip." *The World Fact Book*. https://www.cia.gov/library/publications/the-world-factbook/geos/print_gz.html.

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. 2014. *The NSA Report: Liberty and Security in a Changing World*. Princeton: Princeton University Press.

Cropsey, Seth. 2019. "Hamas Cyber Attack and Israel's Armed Response." *Hudson Institute.* https://www.hudson.org/research/15016-hamas-cyber-attack-and-israel-s-armed-response.

DeIviscio, Jeffery, Diantha Parker, David Furst, Jeff Roth, Jon Huang, and Artin Afkhami. 2017. "Iran, the United States and a Political Seesaw." *New York Times.* https://archive.nytimes.com/www.nytimes.com/interactive/2012/04/07/world/middleeast/iran-timeline.html#/%23time5_206#time5_210.

Demchak, Chris, and Peter Dombrowski. 2013. "Cyber Westphalia: Asserting State Prerogatives in Cyberspace." *Georgetown Journal of International Affairs*: 29–38.

Department of State. 2017. "Foreign Terrorist Organizations." https://www.state.gov/foreign-terrorist-organizations/.

Dipert, Randall. 2010. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9 (4): 384–410.

Dorbolo, Jon. 2001. "Just War Theory." *Oregon State.* https://oregonstate.edu/instruct/phl201/modules/just_war_theory/criteria_intro.html.

Dostri, Omer. 2018. "Hamas' Cyber Activity against Israel." *The Jerusalem Institute of Strategy and Security.* https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/.

Fidler, D.P. 2011. "Was Stuxnet an Act of War? Decoding a Cyberattack." *IEEE Security & Privacy* 9 (4): 56–59.

Finlay, Christopher. 2018. "Just War, Cyber War, and the Concept of Violence." *Philosophy & Technology* 31 (3): 357–77.

Foltz, Andrew. 2012. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate." *Joint Force Quarterly : JFQ* 67: 40–48.

Ford, Shannon Brant. 2013. "Jus Ad Vim and the Just Use of Lethal Force-Short-of-War." *Academia.edu.* https://www.academia.edu/29802902/Jus_Ad_Vim_and_the_Just_Use_of_Lethal_Force_Short-of-War.

Frowe, Helen. 2016. "On the Redundancy of Jus Ad Vim: A Response to Daniel Brunstetter and Megan Braun." *Ethics & International Affairs* 30 (1): 117–29.

Galliott, Jai, and Warren Reed, eds. 2016. *Ethics and the Future of Spying: Technology, National Security and Intelligence Collection.* London, UK: Routledge.

Gates, Guilbert. 2012. "How a Secret Cyberwar Program Worked." *New York Times.* https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?ref=middleeast.

Globes. 2016. "Israel is a Global Cyber Security Power." Consulate General of Israel in Los Angeles. Comments by Prime Minister Benjamin Netanyahu. https://embassies.gov.il/la/NewsAndEvents/Pages/Israel-is-a-global-cyber-security-power.aspx.

Gross, Judah Ari. 2019. "IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle." *Times of Israel.* May 5, 2019. https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/.

Hammes, Thomas X. 2004. *The Sling and the Stone: On War in the 21st Century.* St. Paul, MN: Zenith Press, MBI Publishing Company.

Iasiello, Emilio. 2017. "China's Cyber Initiatives Counter International Pressure." *Journal of Strategic Security* 10 (1): 1–16. http://doi.org/10.5038/1944-0472.10.1.1548.

Johnson, Charles. 2006. "Reuters Doctoring Photos from Beirut?" *Little Green Footballs*. http://littlegreenfootballs.com/article/21956_Reuters_Doctoring_Photos_from_

Kaplan, Shawn. "Are Novel *Jus ad Vim* Principles Needed to judge Military Measures Short of War?" *Academia.edu.* https://www.academia.edu/23697579/Are_Novel_Jus_ad_Vim_Principles_Needed_to_Judge_Military_Measures_Short_of_War.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Kerr, Paul K., John Rollins, Catherine A. Theohary. 2010. "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability." Congressional Research

Service Report for Congress. R41524. https://assets.documentcloud.org/documents/2700120/Document-40.pdf.

Kuru, Huseyin. 2017. "Prohibition of Use of Force and Cyber Operations as 'Force.'" *Journal of Learning and Teaching in Digital Age* 2 (2): 46–53.

Kushner, David. 2013. "The Real Story of Stuxnet." *IEEE Spectrum*. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Langer, Ralph. 2013. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." *The Langer Group.* https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Lewis, Al. 2019. "Houston, We Have a Problem: A Space Force Must First be a Cyber Force." *Modern Diplomacy.* https://moderndiplomacy.eu/2019/05/10/houston-we-have-a-problem-a-space-force-must-first-be-a-cyber-force/.

Liptak, Andrew. 2019. "Israel Launched an Airstrike in Response to a Hamas Cyberattack." *The Verge*. https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike.

Macnish, Kevin. 2016. "Persons, Personhood and Proportionality: Building on a Just War Approach to Intelligence Ethics." Chapter 7, 95–106. *Ethics and the Future of Spying: Technology, National Security and Intelligence Collection*. London, UK: Routledge.

Miller, Steven I., and Fredericks, Marcel. 1999. "How Does Grounded Theory Explain?" *Qualitative Health Research* 9 (4): 538–51.

Moseley, Alexander. n.d.a. "Just War Theory." *Internet Encyclopedia of Philosophy.* Accessed October 10, 2019. https://www.iep.utm.edu/justwar/.

———. n.d.b. "The Philosophy of War." *Internet Encyclopedia of Philosophy*. Accessed October 10, 2019. https://www.iep.utm.edu/war/.

Nakashima, Ellen, and Joby Warrick. 2012. "Stuxnet was Work of U.S. and Israeli Experts, Officials Say." *Washington Post.* https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

National Cyber Strategy. 2018. "National Cyber Strategy of the United States of America." https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Nestoras, A. 2018. "Political Warfare: Competition in the Cyber Era." *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, 4427–36. https://doi.org/10.1109/BigData.2018.8622490.

Orend, Brian. 1993. "Kant's Just War Theory." *Journal of the History of Philosophy* 37 (2): 323–53.

———. 2007. "The Rules of War." *Ethics & International Affairs* 21 (4): 471–76.

Philpott, Daniel. 2016. "Sovereignty." *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/archives/sum2016/entries/sovereignty.

Porche III, Isaac R., Jerry M. Sollinger, and Shawn McKay. 2011. "A Cyberworm that Knows no Boundaries." *RAND National Defense Research Institute.* https://assets.documentcloud.org/documents/2700122/Document-42.pdf.

Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva. 2019. *The Growing Need to Focus on Modern Political Warfare.* Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_briefs/RB10071.html.

Rota, Dominic. 2018. "A Quantum Leap in International Law on Cyberwarfare: An Analysis of International Cooperation with Quantum Computing on the Horizon." *Harvard National Security Journal.* https://harvardnsj.org/2018/11/a-quantum-leap-in-international-law-on-cyberwarfare-an-analysis-on-the-need-for-international-cooperation-with-quantum-computing-on-the-horizon/.

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press.

Schwartau, Winn. 1998. "Something Other Than War." *Cyberwar 2.0: Myths, Mysteries and Reality. Part One: Strategy and Diplomacy*, 55–63. Fairfax, VA: AFCEA International Press.

Schwartz, Felicia, and Dov Lieber. 2019. "Israel, Gaza Trade Blows in Deadly Exchanges." *Wall Street Journal.* https://www.wsj.com/articles/israel-gaza-trade-blows-in-deadly-exchanges-11557052053.

Scott, Helen. 2009. "What is Grounded Theory?" *Grounded Theory Online.* http://www.groundedtheoryonline.com/what-is-grounded-theory/.

Shahaf, Tal. 2018. "Hamas Preparing for Cyber War." *Globes Israel's Business Arena.* https://en.globes.co.il/en/article-hamas-preparing-for-cyber-war-1001246720.

Singer, P.W., and Allen Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Stockburger, Peter. 2016. "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum." *American University International Law Review* 31 (4): 545–91.

Texas A&M School of Law Media. 2015. "Thinking Like a Lawyer." YouTube video, 5:09. https://www.youtube.com/watch?v=0L5d2RAWyZs.

Walzer, Michael. 2006. "Regime Change and Just War/Jean Bethke Elshtain Responds." *Dissent* 53 (3): 103–11.

———. 2015. *Just and Unjust Wars.* 5th ed. New York: Basic Books

———. 2018. "Just and Unjust Leaks: When to Spill Secrets." *Foreign Affairs* 97 (2): 48–51.

Warner, Michael. 2017. "Intelligence in Cyber – And Cyber in Intelligence." In *Understanding Cyber Conflict: 14 Analogies.* Chapter 1, 17–30. Washington, DC: Georgetown University Press.

Weir, Fred. 2015. "To Protect 'Digital Sovereignty,' Russia Threatens to Block Google, Facebook." *The Christian Science Monitor*. Boston, MA: The Christian Science Publishing Society.

Wortham, Anna. 2012. "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent that May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" *Federal Communications Law Journal* 64 (3): 643–60.

Zetter, Kim. 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/