How Cyberspace Changes International Conflict

https://www.e-ir.info/2019/12/08/how-cyberspace-changes-international-conflict/

P.J. BLOUNT, DEC 8 2019

This is an excerpt from *Reprogramming the World: Cyberspace and the Geography of Global Order*. Get your free copy here.

In May of 2013, Cody Wilson printed a working gun with a 3D printer and fired it.[1] Shortly thereafter he made the computer file, that is a set of instructions for a 3D printer to print what he called the Liberator, available online for download. It was downloaded more than 100,000 times before Wilson removed the file.[2] Little did Wilson know that he was running afoul of the United States' International Traffic in Arms Regulations (ITAR). These regulations prohibit the export of "defense items" – in other words, weapons – found on the United States Munitions List (USML) without authorization from the government.[3] ITAR also, significantly, prohibits the export of "technical data" on these items, which is data that would assist the manufacturing of the prohibited item.[4] Wilson's file was in a standard language that would allow anyone with an Internet connection to download it and use a 3D printer to manufacture a gun. The file, since it was on the Internet was downloadable anywhere in the world, and Wilson removed the file from his website when confronted by the U.S. Government.[5] Three years later Wilson's file is still online and freely available through sources like the Pirate Bay.[6] Wilson started a company called Defense Distributed, which now manufactures a product called the Ghost Gunner.[7] This desktop CNC mill will take a block of aluminum and mill a lower receiver for an AR-15.[8] Wilson's product cannot be exported, and the computer file is sold only to United States citizens to keep this product from running afoul of ITAR. Yet this product still effectively digitizes a gun, which lowers barriers to access. The gun that it creates is of high quality, and is a gun that is outside of the regulatory loop; it is an untraceable "ghost gun."[9] And while Wilson is keeping tight control over the "technical data" in the .cad files that allow the machine to manufacture the part, he has open sourced the machine itself so that the plans for the hardware and the software that runs it are freely downloadable.[10] Anyone with these files can develop new design files for the Ghost Gunner, and enable it to make a variety of guns and other items. Defense has been distributed, digitally.

The Ghost Gunner is interesting because it shows the capacity of the state to lose control over violence in two ways. First, it lowers the barriers to the production of the means of violence, which weakens government control over violence. It is legal under U.S. federal law for an individual to manufacture a lower receiver, but it was a time-consuming process and required a high level of skill.[11] The Ghost Gunner makes gunsmithing a plug-and-play venture. Second, and important to the discussion below, it shows that the state no longer has control over the spread of violence at its borders. ITAR is specifically meant to help maintain international peace and security by restricting the export of munitions to countries or persons that might use them for ill. ITAR is directly related to the international project of bracketing war, by cutting off the supply of armaments, and ITAR correlates to regimes such as the Wassenaar Arrangement[12] and the Arms Trade Treaty.[13] These initiatives are mechanisms used to stop the flow of armaments across their borders, which was easy when armaments needed to be carried on trucks. Ghost guns are digitized, just as lethal, and save on the shipping cost.

This chapter investigates how Cyberspace changes the nature of territory by examining how Cyberspace changes international conflict. Schmitt's claim "that law and peace originally rested on *enclosures in the spatial sense*" is particularly salient here as it highlights the role of borders in conflict prevention.[14] In Schmitt's territory-centric conception of international law, war is "bracketed" to locations such that it does not "disturb" the spatial order.[15] This chapter will probe this bracketing of war, and illustrate the diminished importance of the border in constructing

the space of conflict.

The argument here is not meant to be a "dethroning of Clausewitz," but it does argue that Cyberspace dramatically changes the context of international conflict through the subversion of territorial borders.[16] In short, it argues that armed conflict as conceived in the international system is tied to territorial geographies, and that international governance mechanisms that are meant to minimize international armed conflict are structured around this link. The chapter then shows how the concept of cyberwar dislodges conflict from these territorial linkages, which makes the application of norms meant to control international violence ineffective at bracketing it. Section one of this Chapter will use the Stuxnet attack on Iran's centrifuges to analyze how international law has traditionally dealt with war as well as some of the observable gaps in that regime. This section will show how Cyberspace dislodges territory from the governance of international armed conflict. The second section will analyze the role of the international concepts of disarmament and deterrence in limiting cyber conflicts, and it will show that these mechanisms are ill equipped for placing substantive limitations on cyberweapons. Finally, it will use the North Korean Sony hack to show how international politics becomes de-territorialized and distributed in Cyberspace, which means that international conflicts processed through Cyberspace become de-territorialized as well.

Territorial Integrity

At the heart of the post-1945 settlement is the UN charter's Article 2(4), which prohibits "the threat or use of force against the territorial integrity or political independence of any state."[17] This article sought for the first time to create a legal prohibition against interstate armed conflict.[18] Article 2(4) and the UN Charter in general were transformative for international law as it enshrined the state as "the arena within which self-determination is worked out and from which, therefore, foreign armies have to be excluded."[19] For the first time the resort to war, characterized in the Charter as the "use of force," was legally prohibited outside of a few exceptions.[20] Article 2(4) compartmentalizes violence within the borders of a state and gives the state sovereignty over violence within its borders. This compartmentalization, or "bracketing" as Schmitt would call it, is not a new process. The bracketing of war is an act of delineating order from chaos, and Schmitt's project is to show how the international spatial order emerged from the externalization of war. For instance, he notes that during the age of European empires violence was pushed to the peripheries of empires by conceptualizing newly found territories as existing outside of the Western-centric international legal system.[21] Article 2(4) represents a new bracketing of war by conceptualizing every state as an inviolate territory of order. States in this new spatialization were connected to law both internally and, importantly, externally in a legal dynamic between *de facto* control and external recognition.[22]

Art. 2(4) did not change extant borders in a way that was perceptible on a map. Nonetheless, Art. 2(4) did change the content of those borders, and in a very dramatic way. By giving all states an obligation to contain violence within their borders, it also gave all states the right to be free of chaos from outside their borders. Article 2(4) underpins the entire international legal regime, which seeks to contain international armed conflict. The Art. 2(4) prohibition on force is central to *jus ad bellum*, and its goals are further advanced through the *jus in bello* and international disarmament efforts. Cyberspace by recoding borders changes international law's ability to bracket digitized war affecting the nature of international peace and security.

The best place to start to unravel this problem is Stuxnet. Stuxnet presents a clear case for the application and analysis of the law of the use of force in the cyber arena. In 2010, researchers uncovered a computer virus that was propagating itself on computers in Iran.[23] The virus, now known as Stuxnet, was a carefully developed computer program that made its way into computers in the Natanz nuclear facility in Iran. Once there, the malware attacked industrial control systems and executed a program that sped up uranium enrichment centrifuges to damage and destroy them before the end of their expected lifetime. The program itself "displayed a level of technical sophistication and integration never before seen in malware,"[24] and it has been referred to as the "world's first digital weapon."[25] The sophistication of Stuxnet was such that it incorporated four zero-day exploits, and was able to jump an air gap that separated Natanz from the Internet.[26] The program was reportedly developed and released by the United States and Israel as a way to slow the Iranian nuclear program.[27] For the purposes of the discussion below, it is assumed that this is a state on state act, placing it firmly within the realm of the international system, making international law the controlling governance mechanism. This raises the "principle intellectual challenge in the law of

information conflict . . . deciding which areas can be covered by a mere extension of conventional legal principles to cyberspace by analogy, and which require whole new methodologies."[28]

The first question to be asked is whether there has been a violation of Article 2(4). If the United States or Israel had flown a plane across the border and bombed the plant, as Israel did to a Syrian facility in 2007, then there would clearly be a violation of Article 2(4).[29] In this case there was no physical violence in a ballistic sense, however, violence was achieved in a kinetic sense in that the centrifuges themselves were physically manipulated in order to destroy them. The centrifuges were attacked, but it is unclear whether this amounts to a use of force under Article 2(4).[30] *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* Rule 11, states that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[31] *The Tallinn Manual* is an attempt by a NATO group of experts to identify "the law currently governing cyber conflict,"[32] but it notes that "the lack of agreed-upon definitions, criteria, and thresholds for application creates uncertainty when applying the *jus ad bellum*."[33] When compared to a statement by a U.S. defense official on the United States Cyber Strategy, who stated "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," it seems as if at least one of the parties has characterized attacks such as Stuxnet as a use of force.[34] *The Tallinn Manual* experts themselves agreed unanimously that Stuxnet was a use of force that violated international law, but they "split … on whether it constituted an armed attack."[35] This split illustrates the disjuncture that occurs when international law is de-territorialized. The separation of "use of force" from "armed attack," categories that were previously substantially concurrent due to the nature of violence, is indicative of the encounter between international and cyber geographies.

Interestingly, Iran never made any complaint to the relevant UN bodies, and instead opted to maintain a high degree of silence on the matter. Iran's silence is related to its own interests in keeping its nuclear program secret, but it also points to one of the key lessons from Natanz: everyone knows that the United States and Israel were responsible for Stuxnet, but no one can prove it definitively. This is dissimilar from, for instance, U.S. covert involvement in Nicaragua, which the ICJ deemed a use of force.[36] In that case, there were physical border crossings by the U.S. and its warfighting capacity that were observed by witnesses to physical attacks.[37] In the case of Stuxnet, no one saw the attack, yet there is ample evidence pointing the finger at the United States and Israel, e.g. the complexity of programming, the target of the attack, the use of high value zero-day vulnerabilities, and anonymous sources informing journalists. There is, however, no definitive evidence of that fact, and the United States has officially made no statement confirming its involvement resting on the plausible deniability that Cyberspace provides.[38]

Digital computing enables the ability to encrypt communications and to hide the source of cyberattacks. Even if a cyberattack were to be traced to an IP address within a state, that state can claim that it is the victim of a hacker using it as a digital hiding spot or that one of its own citizens is the malefactor for which there is limited responsibility. US DoD acknowledges this potential by noting that "low barriers of entry . . . means that an individual or small groups of determined cyber actors can potentially cause significant damage."[39] In the case of Stuxnet, the virus was feeding information back to servers located around the world.[40] Attribution is a core concept in international law, and for there to be an internationally wrongful act the act must be attributable to a state.[41] The Draft Articles on State Responsibility state that "conduct directed or controlled" by a state is attributable to it, but this requires the establishment of a definitive link that proves such. In Cyberspace such links are hidden by veils of government secrecy, including secrecy classification systems and digital veils of encryption making it difficult to attribute an act to the territory of a state and to the state itself.[42] Attribution is a necessary precondition in international law, but attribution "is an enduring problem" in Cyberspace.[43] The attack, though initiated from some specific geographic point, is experienced as coming from Cyberspace. Cyberspace as an origin for an attack is supported by the military adoption of Cyberspace as a fifth domain.[44]

This fifth domain remains outside of international space, and it obscures the geographic links to the use of force.[45] This creates an obvious problem for stability built around the centrality of a sovereign's territorial integrity in the international system, since international borders no longer separate order from chaos when anonymized weapons can pierce borders and affect physical infrastructure. The plausible deniability enabled by Cyberspace means that states are, in part, relying on the prevalence of non-state actors dispersed around the globe to create noise that covers their tracks. National defense is distributed among a network of indistinguishable actors.

Before moving on from Stuxnet, it is worth noting how this incident reflects on*the jus ad bellum's* counterpart – *jus in bello*. *Jus in bello*, or international humanitarian law (IHL), is not without problems of application, but it does seem that it is more adaptable to cyber conflicts.[46] This is primarily because IHL is not centered on questions of territory. Instead, IHL focuses on humanitarian concerns such as the limitation of pain and suffering for civilians and combatants. It is a *lex specialis* that only applies within the space and time of an international armed conflict.[47] As such, IHL principles are a bit more adaptable to Cyberspace, but they are not without gaps.

For instance, in the case of Stuxnet, it is unclear whether there was an ongoing state of armed conflict that would trigger IHL. Though the attacks occurred over the course of several months, Iran was unaware, and when it became aware it did not respond with force nor through any official channels. Despite the lack of clarity as to whether the rules had been triggered, there is evidence that the programmers of Stuxnet worked hard to make sure that it fell within the legal limits of a weapon. States when developing new weapons technologies are required to give the weapon a legal review to ensure that it is a weapon that can be used lawfully.[48] This review must assess whether the weapon is capable of being targeted at a specific target such that its effects, in terms of collateral damage to civilians, are limited in proportion with the military advantage gained[49] and whether the weapon causes unnecessary suffering.[50] The first thing to note is that this review cannot be done in terms of "cyber-weapons" as a class any more than it can be done of "ballistic weapons" as a class. Instead, the analysis is capability by capability, which is confirmed by a US Air Force Instruction on the legal review of cyber capabilities.[51] What Stuxnet's code revealed is that the programmers went to great lengths to infect only specific computers. Stuxnet was equipped with a kill switch that deleted it if the computer did not match very specific conditions.[52] The "missile" portion of the program replicated itself across computers, but was designed to only release its payload, which targeted industrial control boxes, in the Natanz facility.[53] Though the weapon was released through attacks on networks of private Iranian companies, the damage caused minimal threat to human life or civilian property.[54] The weapon itself was designed to work with precision, but it must be remembered that generally "[c]ollateral damage in Cyberspace has a longer reach than in the physical realm."[55] There are other complications with the application of IHL, many of these are simply that: complications. They change the context of humanitarian principles and make the issues more complicated, but IHL would have means of filling the gaps since the regulatory focus in on human lives. For instance, the issue of who constitutes a combatant becomes more complicated but is a problem that is solvable within the imagination of the IHL framework.

Other rifts are deeper. A critical concern for IHL is the military use of civilian objects. All Cyberspace attacks will depend on the use of civilian infrastructure, but Stuxnet illustrates that state cyberattacks will often do more than just transit commercial networks. In order for Stuxnet to work, it had to take advantage of zero-days. These are vulnerabilities in software that are unknown to the programmer and as a result are not patched.[56] When an individual discovers a zero-day, he or she has a few choices of what to do with that information. Some companies have a bounty system in place to buy zero-days; there is a healthy black market for zero-days; and Governments will also buy them.[57] Stuxnet had an unprecedented number of zero-days in its programming.[58] This means that a government left open vulnerabilities in commercial software with the potential to put a multitude of devices at risk. Stuxnet also used fake security certificates that marked it as genuine, so the software would be accepted by the systems on which it installed itself.[59] These digital certificates are issued by companies that rely on strong encryption in order to verify that a piece of software is from a trusted source. Stuxnet exploited these mechanisms damaging the trust system used to verify software across the Internet.[60] This means that these weapons rely on the maintenance and exploitation of vulnerabilities in the commercial infrastructure that underpins the Cyberspace at a global level.[61] While Stuxnet limited the effects of its attack, another state or entity using similar vulnerabilities might not limit such an attack, a point sharpened when it is recognized that computers similar to those found in Natanz are used to run a great deal of critical infrastructure such as power grids and dams.[62]

Stuxnet is a powerful portent for the international system,[63] and, though some authors wisely note the limitations of cyberwar,[64] Stuxnet is a well-documented example of a computer attack that was used to manipulate and destroy a physical object from afar. What is striking about Stuxnet is the difficulty of placing it squarely within the international legal system. This is because weapons like Stuxnet defy the spatial geography of states. These weapons instead allow states to project force through the alternate geography of Cyberspace, allowing them to skirt around borders as well as the legal regime that supports those borders.

Stuxnet displays vulnerabilities in the Cyberspace infrastructure that individuals rely on globally. With other weapons of this sort (i.e. those that are legal but have global implications such as strategic nuclear weapons) states have turned to methods of disarmament and deterrence as a way to manage international peace and security. These mechanisms, which are meant to lower the risk of an Article 2(4) violation, are the subject of the next section.

Ghost Guns

The atomic bomb dropped on Hiroshima near the end of WWII ushered in a new age of warfare driven by technological advances that far outpaced previous innovation blooms. Nuclear weapons, intercontinental ballistic missile delivery systems, long-range stealth bombers, and military satellite systems all widened the ability of states to project force into the territory of other states. States found themselves in a classic security paradox in which the only way to be more secure is to have more and better weapons than one's adversary leading both parties to actively incentivize their own insecurity.[65] To decrease the risk caused by such paradoxes, states turned to disarmament and deterrence mechanisms in order to implement systems of "reciprocal restraint."[66] As discussed above, ITAR is a domestic implementation of such measures.

Disarmament mechanisms usually come in the form of international agreements that ban the development and use of certain weapons, or limit the number of a particular type of weapon that a state may have.[67] Disarmament mechanisms are underpinned by verification. Verification is the act of verifying whether or not a party is complying with an agreement. The importance of verification to disarmament can be seen in Reagan's signature quip: "trust, but verify."[68] Without verification, disarmament agreements tend to be weak and difficult to negotiate. States have traditionally relied on national technical means (NTM) in these agreements as a form of verification, which consist of satellite observation in addition to other types of remote sensing.[69] NTM was an excellent way to verify nuclear disarmament agreements, and the US and USSR were able to rely on satellite observation as a mechanism for verification since nuclear armaments were by their nature quite large. As a result, NTM worked well in forging compromises between the two states as they sought to securely reduce their nuclear stockpiles. It should be noted that "[b]ecause disarmament treaties go to the heart of national and international security, states are wary of frivolously embarking on new ones that might constrain their options."[70]

Deterrence is a companion to disarmament. Whereas disarmament seeks to reduce the munitions through reciprocal restraint, deterrence is a method of reducing the risk that a state might use those weapons. [71] It is a policy designed to "discourag[e] an adversary from doing something it might otherwise choose to do by manipulating its calculation of cost and benefit."[72] For example, China's current policy of no first use of nuclear weapons is coupled with a stockpile of weapons that would not assure success in a nuclear conflict, but would be able to survive first strike and inflict unacceptable losses on an adversary thereby deterring an attack.[73] Deterrence can also be attained through international agreements. The Anti-ballistic Missile Treaty (ABM Treaty) was an example of such an agreement.[74] The US and the USSR, unable to compromise on the reduction of strategic offensive nuclear weapons agreed on a disarmament treaty that reduced the deployment of defensive systems. The ABM Treaty ensured mutually assured destruction (MAD), a concept that restrains states from engaging in an attack because any such attack will result in their own demise. Thus, the ABM Treaty is an agreement that imposes disarmament in order to achieve mutual deterrence.

Traditionally, disarmament and deterrence have been the primary mechanisms for stemming armed conflict before it happens by placing limits on a state's recourse to force. Unsurprisingly, numerous commentators have turned to these concepts as a way to reduce the threat posed by cyber-attacks and cyber-weapons. Gompert and Saunders argue that there are lessons from nuclear deterrence that could be deployed to foster "mutual restraint" in Cyberspace.[75] Yannakogeorgos and Lowther argue that US policy "suffers from a misperception that cyberspace is a virtual environment and as such, eliminates discussion of territory and sovereignty."[76] They argue that international norms can be developed to solve the attribution problem by holding states culpable for cyberattacks "originating in or transiting information systems within their borders," but they give no indication of why states would agree to such an extraordinary norm.[77]

The problem with these approaches is that they ignore the inherently ambiguous nature of Cyberspace in which

weapons are "in essence an algorithm."[78] As an anonymous hacker put it: "The new global arms race is no longer about who controls the most atomic bombs. It is about who controls/owns the most hackers, botnets, and exploits."[79] Zetter claims that just such a "digital arms race" was launched by Stuxnet.[80] Modern disarmament and deterrence were developed by states to deal with weapons of great magnitude, which have traditionally been rather large. NTM, thus, was an acceptable form of verification, because it gave states a tool through which they could peer into the borders of another state and literally see what that state was doing.[81]

NTM was an effective tool when addressing physical weapons, because it allowed states to maintain their borders, but it is useless in Cyberspace arms control.[82] Cyberspace diminishes "the horrors and costs of war . . . tempting" countries to resort to the anonymity of a Cyberattack.[83] The weapons, if designed properly, are meant to be invisible and non-detectable so that "the origins of the attack is almost always unclear."[84] In the case of Stuxnet, discussed above, the programmers went to great lengths to make the program hide itself from the users of the targeted systems. This undermines verification, which is a reason for treaty failure."[85] The immaterial nature of cyberweapons means that states can avoid having an attack attributed to them, which is a significant reason that states would resort to cyberweapons. The attribution problem is further complicated by the trend of "privatised intelligence and information warfare."[86] As former Director of the NSA, Michael Hayden notes, "applying well-known concepts of physical space like deterrence, where attribution is assumed, to cyberspace where attribution is frequently the problem, is recipe for failure."[87]

Cyber-weapons are by nature covert. They are designed to take advantage of unknown vulnerabilities in computer software and are meant to be deniable by the country that uses them. Stuxnet used security certificates from Taiwanese companies, and the virus reported the data it collected to servers located in a variety of global locations.[88] In fact, it may not have been discovered except for the fact that it caused a malfunction in some non-targeted computers in Iran.[89] As a result, the U.S. and Israel have never acknowledged their involvement in the attack. For all useful purposes, Iran was struck by a ghost gun – an untraceable weapon that lacks materiality.

The problem with these digital ghost guns is that they defy location, and as a result they defy control. For example, cyber-weapons make use of botnets, which are geographically distributed network of infected computers known as bots that are under the control of a single "bot master."[90] Botnets are employed in a variety of nefarious undertakings in Cyberspace as they give the bot master distributed computing power and relative anonymity. Botnets cannot be understood to exist within the bounds of a single state, despite the fact that they act as a unitary whole. International governance, a system structured around the national border, is ill equipped to develop disarmament and deterrence mechanisms to control weapons and activities that ignore these borders. Because Cyberspace is everywhere, cyber-weapons "transform […] a limited physical battlefield to a global battlefield."[91] Disarmament and deterrence, as mechanisms are meant to create less ambiguity in international security by creating information about armaments that states can act on. As Gompert and Saunders note, "the complexity of computer networks, their myriad uses, and the many ways of interfering with them could make reciprocal restraint in cyberspace markedly more difficult than in the nuclear and space domain."[92] Cyber-weapons simply do not fit into these mechanisms for a number of reasons.

First, these weapons are immaterial, making any sort of verification system difficult and any sort of deterrence ineffective. These weapons can fit on a thumb drive and can spread through the Internet with the same ease as a viral meme. This makes verification virtually impossible as the weapon itself is not tied to any sort of infrastructure and is freely portable. Deterrence, on the other hand, which often works on the availability of data about a state's weapons systems, is also precluded. Cyber-weapons rely on vulnerabilities in systems that have not been patched. While disclosing the number and nature of nuclear munitions can have an effect on the strategic maneuvers of other states, the disclosure of a cyber-weapon would lead to a software patch that could render the weapon useless. States developing these weapons are incentivized to keep them covert due to the nature of the technology, and this means that international disarmament and deterrence are not capable of encompassing such technologies.

Second, the plausible deniability that accompanies cyber-attacks is an important limitation on a state's ability to comply with disarmament agreements. The nature of the technology that underlies previous disarmament and deterrence mechanisms is such that the state could effectively maintain control over those technologies. While

history is not without examples of individuals attempting to build nuclear reactors in their garages,[93] the technology was of such complexity and scope that states were able to detect such operations and maintain control over the development and deployment of these technologies. Cyberspace is a technological space that is built around fostering innovation. As a result, this means that "lone hackers" are empowered to develop new technologies built on the logical layer making it "largely the realm of nonstate entities."[94] Innovation is not always a good thing; it has made the "network attack . . . literally a cottage industry."[95] The same innovative open door that has pushed numerous startups, boosts "the power potential of non-state actors."[96] Indeed, one might argue that the only difference between a computer virus and a cyber-weapon is the intent of the user. While commentators have argued that states should be responsible for curbing the activities of their own citizens, this gives little answer to the plausible deniability problem.[97]

Last and certainly not least, cyber-weapons are weapons that subvert territory in a way that other weapons do not. Other weapons must physically cross an international border and exert force or violence after having crossed that border. Cyber-weapons can enter from anywhere and attack physical infrastructure far outside the territory of the attacking state. States lack legal mechanisms for restricting armaments that are ephemeral and locationless, and as a result disarmament and deterrence as mechanisms for slowing the spread of armaments are ineffectual because they are dependent on the assumption that States have control over their borders and the mechanisms of physical violence within those borders.

Cyber-weapons create uncertainty, and uncertainty stands in contrast to verification. Indeed, as seen above with Stuxnet, "the very point of a cyberattack, at least in part, is to increase uncertainty."[98] These weapons render the border ineffectual as a geographic indicator both in their control, as seen here, and their use, as seen with Stuxnet. This means that states are able to exceed their own geography through Cyberspace, giving them more options through which to pursue politics and conflict. The final section of this chapter will address how cyber conflict functions to dislodge international politics from their terrestrial bonds.

Conflict in Black

In May of 2014, the U.S Department of Justice (USDoJ) filed an indictment against what it alleged were five cybercriminals. This in and of itself was not a necessarily novel event, but the individuals charged were novel. The indictment was against five members of the Chinese People's Liberation Army (PLA) who notably operated and resided in China.[99] The USDoJ asserted that these individuals were guilty of economic espionage in Cyberspace. The indictment itself marked a fever pitch in the bickering between the U.S. and China over the limits of online espionage. In this diplomatic impasse, the U.S. argued that China was violating international law by spying on companies for economic advantage and stealing intellectual property.[100] While the U.S. was pressing its concerns, though, Edward Snowden leaked a multitude of documents that revealed the United States' own espionage efforts.[101] When China cried foul, the U.S. drew a line between diplomatic espionage and economic espionage.[102] The indictment from USDoJ was meant to reinforce the international norm that the U.S. was endorsing.

Contrary to the intentions of the U.S., the indictment served to reinforce the vast uncertainties about state action in the Cyberspace. The criminal sanctions, first and foremost, show the inability of the U.S. to stop such actions. While meant more as a diplomatic exclamation point, it must be noted that unless one of the indicted individuals sets foot into the U.S., it is powerless to enforce the law it is invoking. Indeed, the indictment, far from emphasizing a point, seems to reveal the anxiety of the U.S. over its inability to ebb the flow of information to Chinese hackers. It also revealed the morphing nature of diplomacy, espionage, and conflict.[103] Were these military operations? Espionage? Or were they simply criminal acts?

The murkiness caused by state action online results from the attribution issues noted above. The ability of states to effectively conceal their cyber operations gives them great leeway to act in that realm, which is coupled with a low cost of entry.[104] This is important to contemplate because it changes the space in which international politics unfold by changing the territory of war. In simplified terms, states may pursue their goals in international fora through diplomacy (here meant to mean anything that is not war including things like sanctions) or armed conflict. International law serves as a mechanism to keep states pursuing their interests within the confines of diplomatic

action, which is why Art. 2(4) strikes the balance at the heart of international law by focusing on violence that crosses internationally agreed upon boundaries. Cyberspace short-circuits that balance by removing the obstacle of the border and the corresponding risk of identification. States now have a third option of engaging through the geography of Cyberspace to achieve their goals. This third option is marked by the possibility of at once using force and refraining from armed conflict. International politics, as a result, can now be mediated through the geography of Cyberspace.

This can be seen in the hack of Sony Pictures that was first revealed in November 2014.[105] The sophisticated hack affected most of Sony Pictures internal network and the company's internal information (including items such personnel records, e-mails, and unreleased movies) began to be leaked to the public.[106] The attack was soon linked to the upcoming release of the movie *The Interview*, a comedic parody about two Americans assassinating Kim Jong-un, and the attack was assumed to have North Korean ties. When Sony was defiant about releasing *The Interview*, the hack was coupled with threats of terrorism that resulted in Sony pulling the release, though it was subsequently released online and in several theaters.[107] Two days later, on 19 December, the FBI announced that it was attributing the attack to North Korea, though there has been great speculation as to the validity of this attribution.[108] President Obama, on 2 January 2015, imposed sanctions on North Korea, which is the first time sanctions have been used in direct response to a cyber-attack.[109] Throughout this ordeal, the nature and scope of the attack made it a multidimensional threat that challenged the accepted nature of coercive action within the realm of the international.

The initial hack was credited to The Guardians of Peace (GOP) hacker group.[110] This attack was initially seen as a cybercrime against a corporation meaning that the core security concern was the security of Sony's network.[111] As a crime, the criminal is answerable to the state, but the focus is on the private network itself. At first, the hack of Sony did look criminal in nature as the hackers attempted to extort individual employees to keep their personal information from becoming public.[112] However, soon after this, security researchers began to find hints, such as Korean language packs, that linked the hack to North Korea. In a somewhat controversial move, the U.S., and specifically the FBI, attributed the attack to North Korea thus moving the hack into the national security narrative. It also moves the act out of the spectrum of a crime and into the spectrum of international relations, and as a result the U.S. issued sanctions against the North Korean regime.

Superficially, US action in this incident may seem like business as usual in the context of international governance, but a close reading reveals a number of the uncertainties that show how borders are being recoded with new content. As noted above the FBI's attribution was hotly contested by security researchers, but a number of revelations show that even if North Korea was the master puppeteer, the cast of characters taking part in the hack was a globally distributed group of non-state actors. For instance, the Lizard Squad hacker organization may have been involved in the hack as North Korean hired cyber contractors or, possibly, mercenaries.[113] The attribution question leads into a maze where the source of international conflict can no longer be pinpointed to a single site in terms of territory. The capabilities or weapons used are distributed, digital ghost guns making response difficult when the geographic source of the attack is territorially different from the attack, in this case North Korea and Cyberspace, respectively.

A second ambiguity is the nature of the attack. The attack on its face is novel, making it an interesting touchpoint for understanding how Cyberspace changes international space. North Korea bought technology that allowed it to attack a private U.S. entertainment company in an attempt to halt the release of a film within the territory of the U.S., and the attack garnered a response at the executive level in the U.S. In terms of international governance, the attack on Sony raises difficult questions of classification. If the source of the attack was indeed North Korea, it is safe to say that their military was involved, so one might think that this case would resemble the PLA case noted above. Personal information of employees and corporate information and intellectual property were stolen and released online. This has all the trappings of the economic espionage charged in the PLA indictment. The U.S., however, chose a different response, which indicates that they intended to classify this cyber incident in a different category that goes beyond that of domestic criminal law, which is the usual mechanism states use against espionage within their territorial borders. The use of a presidential order for sanctions against North Korea indicates a heightened concern for U.S. national security. Indeed, the president's order states that

provocative, destabilizing, and repressive actions and policies of the Government of North Korea, including its destructive, coercive cyber-related actions during November and December 2014, actions in violation of UNSCRs 1718, 1874, 2087, and 2094, and commission of serious human rights abuses, constitute a continuing threat to the national security, foreign policy, and economy of the United States[114]

There are two factors that heightened the U.S. response in this incident. The first is that the North Korean actions were targeted at denying freedom of speech, a fundamental human right in the view of the U.S., and the second is the additional threats of acts of physical terrorism against theaters that show the movie.[115]

What might be an even more interesting question though, would be how the North Korean authorities envisioned their actions. The regime is notoriously opaque, so ever having a full understanding of the logic that went into these actions is unlikely. North Korea's actions do show how Cyberspace changes the content of international action. Without cyber, North Korea's options would have been to choose diplomacy or conflict. If they choose diplomacy, they have a variety of peaceful options including negotiating with the U.S., placing sanctions on the U.S., or placing sanctions on Sony the company. These options seek to coerce change in another country through indirect action that stays outside of that country's territorial borders. In this case, North Korea could see that these options would be ineffectual due to its relative power in the international community. It could also see that taking action in the form of direct action, i.e. conflict, within the borders of the U.S. is also not an available option due to its relative military power.[116] Cyberspace allowed North Korea to bypass this decision, by giving it the power to take a third path through the geography of Cyberspace. The similarities to Stuxnet as a coercive action should not be ignored. The Sony hack illustrates a second situation wherein a state was able to take direct actions that interfere with a state's "political independence" without the telltale violations of its "territorial integrity."[117]

Similar to Stuxnet, the Sony hack raises questions about thresholds for self-defense under Article 51 and the application of IHL.[118] These regimes are meant to limit state action to the realm of diplomacy but are dependent on the inherent territoriality seen in past conflict. The third path of action allows states the option to exceed their territory and directly encounter the space of an adversary state without geographic movement. The Sony-North Korea hack is one of a growing number of examples that demonstrate how the spatial context in which the international unfolds is being transformed by the imposition of alternate geographies, and it highlights how the nature of Cyberspace challenges underlying assumptions that shape the international space.

—

This chapter has shown how the governance system built around the physical territorial space of the state is being reshaped through the introduction of Cyberspace. This argument is built on illustrating how territorial borders no longer "bracket war" as envisioned in Art. 2(4). The international system, in other words, is ill equipped to create regulatory mechanisms that inhibit and control state action in Cyberspace, much less the myriad other actors that can wield such violence.

This theme of shifting international space will be extended in the next two chapters that address legal and political space. A number of subthemes will become evident as well and are worth noting as the analysis moves forward. First, the role of U.S. action will be used as an explanatory mechanism throughout these chapters. The reason for this is twofold. First, the U.S. was where the Internet originated, and it harbors a bulk of the physical, application, and content layers of the Internet. As such, it is of particular value in examining norm creation, or lack thereof, in Cyberspace. Second, it is hoped that the comparison of various U.S. actions reveals a certain schizophrenia in U.S. policy that indicates an understanding of Cyberspace as something extraterritorial, but an inability to coherently develop an international policy due to its own territoriality.

A second theme is that of attribution. The ability to trace an action back to an actor will recur throughout these chapters. The technology that allows for the concealment of identity will be addressed specifically in Chapter 8's exploration of encryption technologies. Attribution or lack thereof is critical in understanding how Cyberspace allows individuals and entities to transcend their own geographies and take part in other geographies.

Finally, a theme hinted at here that will become more evident in the next two chapters is the role and variety of non-state actors and their ability to contend directly with states in the geography of Cyberspace. This chapter highlighted a state's ability to blend in with the noise of non-state actors. Moving forward this theme will be addressed in terms of the ability of non-state actors to engage globally outside the strictures of the international arena.

Notes

[1] Silverman, "A Gun, a Printer, an Ideology" (2013).

[2] Cadwalladr, "Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian" (2014).

[3] 22 C.F.R. 120 (2019).

[4] 22. C.F.R. 120.6 (2019).

[5] Cadwalladr, "Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian" (2014). *See also* Feuer, "Cody Wilson, Who Posted Gun Instructions Online, Sues State Department" (2015).

[6] Greenberg, "I Made an Untraceable AR-15 'Ghost Gun' in My Office—And It Was Easy" (2015).

[7] *Id.*

[8] Guns are made up of many parts. The lower receiver is the component that is regulated under the US law. *Id.*

[9] *Id.*

[10] Defense Distributed, "Downloads" (2016).

[11] Andy Greenberg, "I Made an Untraceable AR-15 'Ghost Gun' in My Office" (2015).

[12] Wassenaar Arrangement, "About Us" (2016).

[13] Arms Trade Treaty (2014).

[14] Schmitt, *Nomos of the Earth* (2003).

[15] *Id.* at 186.

[16] Betz, "Clausewitz and Connectivity" (2013). *See also* Betz & Stevens, *Cyberspace and the State* (2011) 12.

[17] UN Charter (1945) 2(4).

[18] *See generally*, Pompe, *Aggressive War – An International Crime* (1953) 12, 160–64.

[19] Walzer, "The Moral Standing of States" (1980) 210.

[20] For those exceptions *see* UN Charter (1945) Art. 42 & 51.

[21] Schmitt, *The Nomos of the Earth* (2003) 101–125.

[22] *See generally* Coicaud, "Deconstructing International Legitimacy" (2009) 29–86.

[23] *See generally,* Zetter, *Countdown to Zero Day* (2014) Chap. 1.

[24] Oliver, “Stuxnet” (2013) 129.

[25] Zetter, *Countdown to Zero Day* (2014) 3.

[26] Oliver, “Stuxnet” (2013) 143.

[27] Broad, Markoff, & Sanger, “Stuxnet Worm Used Against Iran Was Tested in Israel” (2011).

[28] Wingfield, “Legal Aspects of Offensive Information Operations in Space” (1998) 1.

[29] Zetter, *Countdown to Zero Day* (2014) 192, 215–216.

[30] *See* Kallberg & Burk, “Cyberdefense as Environmental Protection” (2013) 265–75.

[31] Schmitt, ed., *Tallinn Manual* (2013) 45.

[32] *Id.* at 5.

[33] *Id.* at 42. *See also* Libicki, “Two Maybe Three Cheers for Ambiguity” (2013) 30 and Dipert, “The Essential Features of an Ontology for Cyberwarfare” (2013) 35–48.

[34] Gorman & Barnes, “Cyber Combat” (2011). *See also* Sanger & Bumiller, “Pentagon to Consider Cyberattacks Acts of War” (2011) and Friedman & Preble, “A Military Response to Cyberattacks Is Preposterous” (2011).

[35] Zetter, *Countdown to Zero Day* (2014) 402.

[36] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (1986) 14.

[37] *Id.* at para. 22.

[38] McDermott, “Decision Making Under Uncertainty” (2010) 234 and Edward Snowden, “Testimony before the Parliament of the European Union” (2014) 4.

[39] US DoD, “Department of Defense Strategy for Operating in Cyberspace” (2011) 3.

[40] Zetter, *Countdown to Zero Day* (2014) 27.

[41] Draft Articles on the Responsibility of States for Internationally Wrongful Acts (2001) Art. 2.

[42] *See generally* Clark & Landau, “Untangling Attribution” (2010).

[43] Zetter, *Countdown to Zero Day* (2014) 64. *See generally* Allan, “Attribution Issues in Cyberspace” (2013) 55–201.

[44] US DoD, “Department of Defense Strategy for Operating in Cyberspace” (2011) 5.

[45] *Id.* at 8 and Department of the Army, “FM 3-38: Cyber Electromagnetic Activities” (2014) 1–4.

[46] Dunlap, “Perspectives for Cyberstrategists on Cyberlaw for Cyberwar” (2013) 212. *See also* Department of the Army, “FM 3-38: Cyber Electromagnetic Activities” (2014).

[47] Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (2004) 1–16.

[48] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1977) Art. 36. *See also* Blount, "The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons" (2012) 11–20.

[49] Gompert & Saunders, *Paradox of Power* (2012) 126

[50] *See generally* Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (2004) 80–82.

[51] United States Air Force, Legal Reviews of Weapons and Cyber Capabilities, A.F. Instruction 51–402 (2011).

[52] Kim Zetter, *Countdown to Zero Day* (2014) 59.

[53] *Id.* at 52.

[54] *Id.* at 388.

[55] *Id.* at 382. 352. On targeting in cyberspace see Department of the Army, "FM 3-38: Cyber Electromagnetic Activities" (2014) 3–12.

[56] Zetter, *Countdown to Zero Day* (2014) 6.

[57] *Id.* at 13.

[58] Oliver, "Stuxnet" (2013) 129.

[59] Zetter, *Countdown to Zero Day* (2014) 13.

[60] *Id.* and DeNardis, *The Global War for Internet Governance* (2014) 95.

[61] Gompert & Saunders, *Paradox of Power* (2012) 142; Taylor & Carter, "Cyberspace Superiority Considerations" (2013) 14.

[62] Zetter, *Countdown to Zero Day* (2014) 61–62

[63] Oliver, "Stuxnet" (2013) 128. *See also* Zetter, "Everything We Know About Ukraine's Power Plant Hack" (2016).

[64] Lee & Rid, "OMG Cyber!" (2014) 4–12.

[65] Gompert & Saunders, *Paradox of Power* (2012) 1–12.

[66] *Id.* at 115.

[67] Disarmament mechanisms are not always necessarily "legal" documents. Transparency and confidence building measures (TCBMs) that facilitate information sharing among states, such as the Hague Code of Conduct on Ballistic Missile Activities, also serve the project of disarmament. *See generally* Hague Code of Conduct against Ballistic Missile Proliferation (2002).

[68] Harrison, *Space and Verification, Volume I* (2007).

[69] Morgan, "Deterrence and First-Strike Stability in Space" (2010) 9–11.

[70] Findlay, "Why Treaties Work, Don't Work and What to Do About It?" (2006).

[71] Morgan, “Deterrence and First-Strike Stability in Space” (2010) 23.

[72] *Id.* at 24.

[73] Gompert & Saunders, *Paradox of Power* (2012) 39–67.

[74] Treaty Between The United States of America and The Union of Soviet Socialist Republics on The Limitation of Anti-Ballistic Missile Systems (ABM Treaty) (1972).

[75] Gompert & Saunders, *Paradox of Power* (2012) 115–150.

[76] Yannakogeorgos & Lowther, “The Prospects for Cyber Deterrence” (2013) 50

[77] *Id.* at 51.

[78] Dipert, “The Essential Features of an Ontology for Cyberwarfare” (2013) 36. *See also* Rowe *et al*., “Challenges in Monitoring Cyberarms Compliance” (2013) 81.

[79] Prisoner #6, “The 21st Century Hacker Manifesto” (2014–2015) 50. *See also* Department of the Army, “FM 3-38: Cyber Electromagnetic Activities” (2014) 3–11

[80] Zetter, *Countdown to Zero Day* (2014) 370.

[81] Sanger & Bumiller, “Pentagon to Consider Cyberattacks Acts of War” (2011).

[82] Zetter, *Countdown to Zero Day* (2014) 400.

[83] *Id.* at 375.

[84] Sanger & Bumiller, “Pentagon to Consider Cyberattacks Acts of War” (2011).

[85] Findlay, “Why Treaties Work, Don’t Work and What to Do About It?” (2006) 4.

[86] Singer, *Corporate Warriors,* 99 (2011) 101. *See also* Scahill, *Blackwater* (2007) 415.

[87] Hayden, “The Future of Things Cyber” (2013) 4. *But see* Chen, “An Assessment of the Department of Defense Strategy for Operating in Cyberspace” (2013) 6.

[88] Zetter, *Countdown to Zero Day* (2014) 28.

[89] *Id.* at 7–8.

[90] *See generally* Maurushat, “Zombie Botnets” (2010) 370–83.

[91] Department of the Army, “FM 3-38: Cyber Electromagnetic Activities” (2014) 1–5.

[92] Gompert & Saunders, *Paradox of Power* (2012) 115.

[93] *For example* Aaronson, “The DIY Engineer Who Built a Nuclear Reactor in His Basement” (2014).

[94] Gompert & Saunders, *Paradox of Power* (2014) 131, 117.

[95] *Id.* at 133.

[96] Betz & Stevens, *Cyberspace and the State* (2011) 11.

[97] *See for example* Gompert & Saunders, *Paradox of Power* (2014) 117 and Sofaer *et al*., "Cyber Security and International Agreements" (2010) 190.

[98] McDermott, "Decision Making Under Uncertainty" (2010) 229.

[99] U.S. v. Wang *et al*. – *Indictment* (W.D. Penn. 2014).

[100] *See also*, Brenner, "Gray Matter" (2013) and U.S. v. Wang (2014) para. 5.

[101] *See* Carroll, "Barack Obama and Xi Jinping Meet as Cyber-Scandals Swirl" (2013); White House, "PPD-20: U.S. Cyber Operations" (2013); and Zetter, *Countdown to Zero Day* (2014) 369.

[102] Spying, for national security reasons, is generally considered legal under international law. Gompert & Saunders, *Paradox of Power* (2012) 140–141. *But see* Snowden, "Testimony before the Parliament of the European Union" (2014) 8.

[103] Lucas, "Can There Be an Ethical Cyber War?" (2013) 201.

[104] US DoD, "Department of Defense Strategy for Operating in Cyberspace," (2011) 3.

[105] Weisman, "A Timeline of the Crazy Events in the Sony Hacking Scandal" (2014).

[106] *Id.*

[107] Richardson, "Sony kills 'The Interview' after North Korea hack, terror threat" (2014).

[108] FBI Press Office, "Update on the Sony Investigation" (2014). *But see* Lee, "The Feds Got the Sony Hack Right, But the Way They're Framing It Is Dangerous" (2015); Schneier, "Attributing the Sony Attack" (2015); Goldsmith, "The Sony Hack" (2014); and Sexton, "Accurately Attributing the Sony Hack Is More Important than Retaliating" (2015).

[109] White House, Executive Order – Imposing Additional Sanctions with Respect to North Korea (2015).

[110] Weisman, "A Timeline of the Crazy Events in the Sony Hacking Scandal" (2014).

[111] *Id.*

[112] *Id.*

[113] Diaconescu, "Inside Job" (2014).

[114] White House, Executive Order – Imposing Additional Sanctions with Respect to North Korea (2015).

[115] Sneed, "Sony Hack Takes Darker Turn" (2014).

[116] *For example* Fish, "Could North Koreans Ever Really Invade America?" (2012).

[117] UN Charter (1945) Art. 2(4).

[118] *See generally* Schmitt, "Cyber Operations in International Law" (2010) 151.

About the author:

P.J. Blount is a Post-doctoral researcher at the University of Luxembourg in the Faculty of Law, Economics, and Finance. His research focuses on space and communications law. Previously he served as a Research Counsel and Instructor at the University of Mississippi School of Law; was a Visiting Scholar at the Beijing Institute of Technology, School of Law; and an Adjunct Professor at Montclair State University, Department of Political Science and Law.