The Cyber Defense Review

Research Articles

The Violence of Hacking: State Violence and Cyberspace

Dr. Aaron F. Brantly

The violence of bits and bytes is real. How can we conceive of violence in a digital world? Do traditional definitions provide a reasonable means to understand the impact of violence emanating from cyberspace? This work examines the concept of violence at the state level and builds and argument that violence is not confined to pre-digital static definitions. Like physical violence, cyber violence conducted by states is instrumental and constitutive of both physical and non-physical acts. These acts in combination facilitate state goals, specifically the potential to win wars or achieve related policy objectives. Cyber war is not your father's war, but it has many of the same effects. What are the first, second and third order effects achievable in cyberspace? Are these effects conceptual or have they been demonstrated? What does and can state violence in cyberspace look like and why is it important?

violence *noun* | vi·o·lence : behavior involving physical force intended to hurt, damage, or kill someone or something. [1]

Outside of academia, the definition of violence is broad and far reaching. The word violence typically conjures up very physical and direct notions of the application of force. The World Health Organization defines violence as: "the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either result in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation." [2] The language used to identify violence is straightforward, or so it seems. Over the last several decades and in particular the last ten years a new form of violence has risen to the forefront of global consciousness. Cyber violence can be constitutive of both physical and non-physical, threatened and applied forms of violence. Concepts of cyber violence run headlong into historical semantic debates on the use and value of words extended beyond their core definition.

Dr. Aaron F. Brantly is Assistant Professor of International Relations and Cyber in the Departments of Social Sciences and Electrical Engineering and Computer Science, Cyber Policy Fellow at the Army Cyber Institute and Cyber Fellow at the Combating Terrorism Center at the United States Military Academy. He holds a Ph.D. in Political Science from the University of Georgia and a Master's of Public Policy from American University. His research focuses on national security policy issues in cyberspace including big data, terrorism, intelligence, decision-making and human rights. His most recent book is *The Decision to Attack: Military and Intelligence Cyber Decision-Making* published by the University of Georgia Press.

Many scholars with static semantic approaches to the development of theory claim that cyber violence is not violence as expressed by definition, but something more akin to subversion or manipulation. Semantics aside, violence emanating from cyberspace is a misunderstood concept. Whereas most forms of violence are constitutive of direct or threatened applications of physical force, cyber violence does not often possess a direct causal relationship with the force it creates. Assessing the use of violence by states has long been a core aspect of the study of International Relations (IR). As a field of study international relations privileges the use of concrete language and "good" research methods to identify relationships between phenomena.[3] Within IR even the most hard and fast theories, those rigorously developed and defended over scholarly careers are often under constant and sustained challenges from novel explanations for phenomena.

Rather than being a hard science in which there are laws governing the interaction of phenomena, social sciences largely remain in theory. Scholars test theories over and over, compare them with better explanations for phenomena and then attempt to maintain a hard core of a theory through a positivist heuristic.[4] This paper argues that the definition of violence by states against states is limiting. The present static semantic approach to language within the existing theoretical core focuses on first-order effects of violence to the exclusion of valid and significant second and third order effects not foreseen by original theorists. The semantic rigor associated with the core of many theories obfuscates the reality of most acts of state violence. As the world becomes increasingly digitized and the science fiction of yesterday becomes the science fact of today, it is necessary to incorporate a more encompassing explanation of violence into

IR scholarship. The realization of violence as a complex phenomenon not confined to use or threatened use of physical acts will establish a novel basis for understanding a broad range of legal and policy concepts related to cyber actions as well as more robust models of compellence and deterrence. As the term evolves to encompass actions in new domains of war-fighting, it is necessary to expand the core epistemological foundation upon which we examine novel actions. The semantic understanding of violence is historically relevant, yet its value and importance moving into the future loses utility when explaining new phenomena. Cyberspace is a violent domain. It is violent both in its ability to affect physical violence through first, second and third order effects, but also in its ability violently alter the reality of the world in which we exist in the present. William Gibson wrote of cyberspace as a:

> ... consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphical representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters, and constellations of data. Like city lights, receding. [5]

Although the concept of violence in cyberspace is rooted in theoretical foundations and historical semantics, it should not remain static. Despite the semantic and theoretical core, a positive heuristic predicated on modifications to the existing meaning of violence serves to retain the core attributes of the word while expanding its definition to include those acts that are not directly physical. A historically rooted theory based approach is insufficient for an understanding violence in this domain. To understand violence as it pertains to hacking, we must also examine the fundamentals of code, the development of national mission teams and the evolution of society towards a new consensual hallucination, one in which physical and digital violence are linked by the code upon which our lives increasingly depend. The argument below specifically focuses the application of violence through the use of cyberspace as a means to highlight the gaps in present interpretations of law and policy.

Defining Instrumental Violence in War

war *noun* | \'wȯr\ : the state of armed conflict between different nations or states or different groups within a nation or state. [7]

States have a history of violence. This violence can manifest in many forms. Yet, violence is by its nature is instrumental. [6] War defined as "the state of armed conflict between different nations or states or different groups within a nation or state" constitutes the application of violence on the largest scale. [7] In focusing on the history of violence by states, I confine this study to the application of violence in the form of war and examine the usage of violence by states for the purpose of achieving political utility. [8] Waltz and

other realist theorists contend that war arises out of an absence of an overarching control on a system of anarchy in which states interact.[9] The subsequent use of physical force is intended for the preservation of the survival of the state. As states seek to rigorously establish their security they degrade the security of other states within the system.[10] In its attempts to establish security, the state need not necessarily apply violence, but merely the threat of violence or rather the potential to achieve violence can serve to reduce the security of other states. While realists contend that the focus of this violence is necessarily located in physical security at the top of a needs hierarchy, liberals and in particular, neoliberal institutionalists, contend that the hierarchy of needs is not isolated to the use of physical violence but also to activities that might threaten the survival of a state over time.[11] The threat of violence can and often is a psychological function predicated on the likelihood of survival.

While physical manifestations of force necessarily establish the historical foundations of violence from cavemen to the present. These manifestations have often been paired with the application of threatened force that denies or disarms an enemy through direct action. Thomas Schelling writes: "Forcible offense is taking something, occupying a place, or disarming an enemy or territory, by some direct action that the enemy is unable to block."[12] Violence is the instrumental means by which to achieve an end. While it is likely that Schelling never considered the forcible occupation or disarmament of an enemy or territory absent physical violence, his definition leaves open the use of non-kinetic means to achieve the same ends.[13]

Concepts of cyber violence run headlong into historical semantic debates on the use and value of words extended beyond their core definition.

By constraining the study of violence to the physical world, we ignore the impact of other manifestations of violence that achieve the strategic, tactical and operational objectives that were once only achievable through physical means. While there remains contention on the impact of non-physical violence, there are studies that suggest that alterations in trade and tariff behaviors can increase the likelihood of physical conflict.[14] The denial of assets to a state in the form of a blockade can include either physical or digital forces intended to hurt an opposing state. The siege of Vicksburg is an example of the physical manifestation of the denial of resources to an opposing force.[15] This denial can weaken an opposing force and while a siege or a blockade can be intensely physical and include directed death and destruction from a cannon, muskets, trebuchets and other weapons of war, the forced isolation of group can result in indirect violence through starvation and disease. Economic actions absent physical actions can also result in indirect violence. The closure of markets, the prevention of the sale of goods and services and the disruption of capital flows can

hurt an opposing state both physically and psychologically. The generation of second order violence that is not the result of a kinetic action but rather the change in policy or the manipulation of markets is violence and can achieve similar effects.

Violence at its most basic is a physical act. Yet, the application of violence by states need not be physical. There are numerous instances of historical violence perpetrated by states that had less to do with a physical action-reaction causal chain than a linkage between the non-physical instigator of violence (policy, law, code, or position) and a resultant pain, damage, or death of the target. The policies of forced collectivization under Stalin resulted in the losses of millions of lives. [16] The semantic interpretation of the violence of Holodomor would be that of physical violence executed by the soldiers. However, these soldiers were rather a manifest instrument of state violence in the form of policy enforcement. If semantic nuance is to be applied to Holodomor, it would likely absolve the state of culpability in the actions of its soldiers. Based on law and interpretations of responsibility for violent acts, the state retains its authority over those who conduct violence in its name. When a murder occurs police do not absolve the murderer if he used a gun. Despite the disconnect in both physical and temporal space between the action, pulling the trigger, and the effect, a bullet entering and harming a victim, the two parts of the causal chain are linked inexorably.

The generation of second order violence that is not the result of a kinetic action but rather the change in policy or the manipulation of markets is violence and can achieve similar effects.

The examples above establish that violence is not merely the physical action-reaction relationship it is made out to be. In neither case was the force that injures a person or thing directly physically connected to its origin at the time at which the violence was affected. While the result was indeed a physical result: pain, damage, or death; the instigation of that result can be both physical and non-physical.

Carl von Clausewitz's examination of violence is not confined to physical manifestations as scholars such as Thomas Rid and others have suggested. Rid contends that "Unless physical violence is stressed, war is a hodgepodge notion." [17] Rid goes on to discuss the necessarily instrumental nature of war as defined by Clausewitz. Even Clausewitz notes that violence in war is not tied to the basest of definitions. The instrumentality of violence in the service of an aim is still present.

Clausewitz writes:

> Its violence is not of the kind that explodes in a single discharge but is the effect of forces that do not always develop in exactly the same manner or to the same degree. At times they will expand sufficiently to overcome the resistance of inertia or friction; at others, they are too weak to have any effect. War is a pulsation of violence, variable in strength and therefore variable in the speed with which it explodes and discharges its energy. [18]

pulsation *noun* | pul·sa·tion : [1] the rhythmical throbbing or vibrating or [2] a periodically alternate increase and decrease of quantity (as pressure, volume, or voltage). [19]

Clausewitz locates war as a continuum of violence (i.e. a pulsation). Pulsation defined as [1] the rhythmical throbbing or vibrating or [2] a periodically alternate increase and decrease of quantity (as pressure, volume, or voltage).[19] Total war is not total physical violence, but violence directed to achieve an aim. To achieve this aim pressure is applied differently at different locations. The application of this pressure in the form of violence can often be more effective if it deprives an enemy of their ability to trust the reality in which it exists. The alteration of the calculus of war manipulates the bargaining range of any given conflict and can result in a preferential outcome for the party best able to leverage violence.[20] The bargaining range of states is affected by more than simple brute physical violence. While physical violence can provide a great deal of information, the manipulation or destruction of information streams necessary to assess one's position within the bargaining range can alter a state's perception on what it stands to gain or lose. The manipulation of the information can shift the bargaining range of states.[21] This is not violence in the brutish sense of old but rather violence of the shared information sphere.

Clausewitz again offers support for a more nuanced assessment of violence as a function of war:

> If for the moment we consider the pure concept of war, we should have to say that the political purpose of war had no connection with war itself; for if war is an act of violence meant to force the enemy to do our will its aim would have always and solely to be to overcome the enemy and disarm him. [22]

The object of state violence in the form of war is not aimless, as Clausewitz indicates it is directed towards the achievement of a political objective. This political aim is often the removal of the ability of an adversary to take up arms, while at other times it is the removal of the will of an adversary to fight. In countering Rid's arguments of constraining violence, John Stone writes "the term 'damage' implies that violence may be directed at artifacts as well as people."[23] Stone rightly identifies that violence against artifacts necessarily extends the concept of violence and increases its instrumental value. The elimination of

artifacts such as bridges, defense manufacturing centers, and any number of strategic or tactical assets demonstrates the value of applications of violence in pursuit war aims.

Robert Pape notes that when examining strategic bombing there are two major types of coercive air options strategic and interdiction.[24] The first targets military, industry or civilian targets with political or economic value and the second focuses on the lines of supply and logistics. It is here where we see kinetic operations as violence in pursuit of the aims of war. These supply lines, once organized and established via paper and person were susceptible only to kinetic violence. The interdiction of these lines through bombing reduces the effectiveness of military operations. The interdiction of logistical networks in modern warfare is likely to achieve a similar effect.

The dictionary definition of violence is pre-digital. This section illustrated the contradictions and short-sighted applications of the classic dictionary definition of violence in the context of modern warfare. The evidence presented in this section extends the concept of violence from the IR theory outward to its ability to achieve strategic, tactical, operational objectives for political purposes. The remainder of analysis picks up where this one leaves off by examining incidents of non-kinetic violence. The analysis serves to situate cyber violence in a modern, nuanced debate. By establishing the impact of cyber violence, scholars and decision-makers are more likely to thoughtfully examine acts of violence emanating from cyberspace and places them within or extend existing theoretical, legal and policy frameworks.

Establishing The Violence of Hacking

hack *noun* | \'hak\ : use a computer to gain unauthorized access to data in a system.[25]

Our survival in much of the industrialized world is predicated on the systems we have established to manage everything from the mundane all the way up to critical infrastructures that run our electricity, our water systems, financial networks and food distribution. Gibson's allusion to a consensual hallucination might not be entirely realized, but as a society, we are rapidly advancing down the path towards full integration. The most basic realization of our integration is the absence of fiat currency in our bank accounts. The value of our savings are not stored as dollars or euros in bank vaults but as zeros and ones magnetized onto hard disks. IR literature places a great deal of emphasis on the physical security and the creation of armies, walls, fortifications and other instruments of war that pose both offensive and defensive threats to others, yet there has been substantially less discussion across the discipline on the creation of cyber units by states to undermine the societal structures upon which we depend.

Arguably many of the same activities, to include physical violence can be achieved through first, second and third order effects generated in and through cyberspace. The optimal code execution for violent effect is in and of itself a unique field of study. Below are a series of case examples that serve to highlight the many ways in which code can function in similar ways to conventional kinetic violent acts. The intent is to open the aperture of theorists and policy-makers to the reality of the present and the world to come. Each example is illustrative not of a theoretical possibility but a demonstrated incident in which code affected violence. By understanding how code can affect violence, we are better able to ascertain its strategic, tactical and operational impact in warfare situations. This should provide limited insight into possible uses by adversary states and sub-state actors. It should also highlight the limitations of current theory, law, and policy.

Digital Interdiction of Supply Lines

Our survival in much of the industrialized world is predicated on the systems we have established to manage everything from the mundane all the way up to critical infrastructures that run our electricity, our water systems, financial networks and food distribution. Gibson's allusion to a consensual hallucination might not be entirely realized, but as a society, we are rapidly advancing down the path towards full integration. The most basic realization of our integration is the absence of fiat currency in our bank accounts. The value of our savings are not stored as dollars or euros in bank vaults but as zeros and ones magnetized onto hard disks. IR literature places a great deal of emphasis on the physical security and the creation of armies, walls, fortifications and other instruments of war that pose both offensive and defensive threats to others, yet there has been substantially less discussion across the discipline on the creation of cyber units by states to undermine the societal structures upon which we depend.

While the scale of violence has shifted in its shock and awe to a point and click the resultant effect is no less severe.

Robert Pape in his article *Bombing to Win* identified different methods of leveraging air power to achieve strategic and tactical objectives. What if the interdiction of supply lines did not require air power at all? What if a state could hack into the supply chain and change orders, destinations of orders, the component attributes of the manufactured supplies and more? Our military is heavily dependent on automated ordering and supply systems distributed across hundreds, if not thousands of contractors and subcontractors, each with a role in facilitating the mission of operational readiness. The introduction of doubt, the reduction in efficiency, the degradation of quality of any given aspect of this supply process could achieve significant impacts. The prospect of an adversary hacking into the US supply and transportation infrastructure for the Department of Defense (DoD) is not speculation, but a present reality.

In April 2013, the Senate Armed Services Committee (SASC) initiated an inquiry into the extent and scope of advanced persistent threat (APT) penetrations into the U.S. Transportation Command (USTRANSCOM). USTRANSCOM's mission is to provide full-spectrum global mobility solutions and related enabling capabilities for supported customers' requirements in peace and war. As one of the nine combatant commands, USTRANSCOM is responsible for managing people trucks, trains, railcars, aircraft, ships, information systems and infrastructure as well as more than 1,203 aircraft and 379 vessels in the Civil Reserve Air Fleet (CRAF) and the Voluntary Intermodal Sealift Agreement (VISA). [26] The Army, The Navy, and the Air Force provide the soldiers, sailors and airmen, but USTRANSCOM gets them to where they need to go and ensures they have the right equipment when they get there. The manipulation of USTRANSCOM in a time of conflict would severely degrade the functional capacity of the US military.

The SASC Report notes that there were at least 20 successful penetrations constitutive of APTs. [27] An APT is a long-term penetration requiring significant and persistent actions by an adversary. While nearly all of these APTs were identified by the FBI, Air Force Office of Special Investigations, the Defense Security Service or the Defense Cyber Crime Center, USTRANSOM was only aware of two. [28] The SASC report notes major failures in information sharing between various government agencies and a fundamental lack of mutual understanding on contractual obligations to share information associated with penetrations into contractor networks.

> Although the effectiveness of STUXNET has received mixed reviews, the ability to damage, disrupt, destroy, and degrade via code is not in doubt.

The penetrations were directly tied to Chinese actors and are in line with China's information operations strategies as outlined in numerous sources. [29] The moves into the transportation and logistics architecture of the DoD has profound ramifications that could undermine the infrastructures established to enable US war-fighting capabilities. The SASC report is careful in its identification of known vulnerabilities and reiterates on multiple occasions "of the at least" indicating that the actual number of penetrations likely exceeded 20. The challenges highlighted by the USTRANSCOM hack are not solely technical, but are illustrative of the challenges faced by multiple overlapping layers of bureaucracies and a strong disincentive on the part of companies to disclose vulnerabilities or exploitations of their platforms for fear of losing position within the lucrative contractor market. The significance of the vulnerabilities highlights that there are violent actions in the form of adversarial actors actively penetrating and seeking to manipulate the critical supply chains necessary for national defense. Objectives once only accomplished by the delivery of tons of munitions are now executed by lines of code with limited risk. While the

scale of violence has shifted in its shock and awe to a point and click the resultant effect is no less severe.

The Aurora Experiments and STUXNET Precision Guided Code

Precision-guided munitions are a novelty in the historical lineage of warfare. They serve to hone the lethal focus of an offender onto an objective of importance. This isolation of target facilitates compliance with the Laws of Armed Conflict, in particular, the Geneva Conventions. Precision guided munitions attempt to protect non-combatants from the horrors of war. While mistakes cannot be not entirely avoided they can be minimized and violence can be more appropriately directed against those willingly engaged in conflict. [30] From a conventional arms perspective precision is defined as "The ability to locate and identify a target, strike it accurately in a timely fashion, and determine whether desired effects have been achieved or a restrike is needed." [31]

Markham Schmitt writes:

> Precision lies at the heart of both contemporary air warfare and the law of armed conflict rules that govern it. Precision capabilities increase an attacker's ability to distinguish between military and civilian objectives, thereby fostering compliance with the principle of distinction. [32]

While using precision guided munitions to foster distinction between combatants and non-combatants in the kinetic physical domains of land, sea, air, and space is not without its challenges, the distinction between civilian and military targets in cyberspace is immensely difficult to discern.

While there is no way to fully eliminate the ability of an armored platform like an M1A2 Abrams from firing, the ability to damage its maneuverability or firing efficiency is a real possibility.

The Idaho National Laboratories on March 4, 2007, demonstrated what is now one of the best-documented executions of precision code. Documents declassified by the Department of Homeland Security indicate that the demonstration was initiated after the discovery of a vulnerability known as "Aurora" in the industrial control systems of "spinning machines (generators, compressors, etc.) that are directly coupled to the electric power grid." [33] The test, which cost $2.876 million was designed to highlight vulnerabilities in the nation's critical infrastructure. [34] The test, conducted against a 27-ton diesel generator, demonstrated the impact of targeted code against industrial machinery and resulted in extensive damage and a total loss of generating capability within three minutes. [35] Video of the incident shows the generator violently shaking and billowing black smoke. The code

functioned to prevent the safety systems (breakers) of the generator from stepping in. What is most profound about this test is not the test itself in isolation, but the realization that the vulnerability was pervasive across thousands of critical infrastructure nodes. [36]

The demonstration indicated a rapid need for enhanced mitigation of vulnerabilities across the national critical infrastructure and spurred DHS to work jointly with multiple industries through Sector Coordinating Councils. What once would have only been achievable using kinetic weapons leveraging either air power or manned sabotage became a digital reality of cyberspace operations. The ability to affect violence on those systems which run and maintain a society's functional order were found to be susceptible to code manipulations.

The Aurora Generator test was only the first in a series of famous hacks to demonstrate the precision and violence of code. In what is now the most famous cyberattack in history, more so than even the original Morris Worm, is the STUXNET Trojan. STUXNET did not manipulate a single code base but rather multiple interdependent systems each with responsibilities safeguarding the enrichment process of uranium gas into Highly Enriched Uranium (HEU). Although discovered by Sergey Ulasen from VirusBlokAda, the first major write up of STUXNET came from Nicolas Falliere, Liam Murchu and Aric Chien of Symantec. [37]

Whereas the Aurora generator test was conducted in a wholly contained environment under strict conditions, all evidence related to the STUXNET attack pointed towards state involvement. [38] The code leveraged an unprecedented four zero-day exploits in a single weapon system. The code itself was highly targeted and focused its attack against a specific brand of Siemens centrifuges using specific software installations language packs and hardware schematics. [39] The cyber weapon system, STUXNET, is the most complex and integrated hacking incident purported to be conducted by a state actor(s). For this article, what should stand out is its discriminating application of violence. The use of code to damage physical systems and to disrupt their production quality removes the brutishness violence and follows more in line with Sun Tzu than Clausewitz. Whereas a bomb offers its violence in a kinetic reaction, code installs its violence in the underlying logical structure that makes things work. Although the effectiveness of STUXNET has received mixed reviews, the ability to damage, disrupt, destroy, and degrade via code is not in doubt.

Economic Warfare Via Code

There is a plethora of instances in which states in a time of war have attempted to undermine the economic viability of their adversary. During the Revolutionary War, the British recognized the importance of finance for the conduct of war. [40] To undermine the American effort, the British deliberately set about undermining the financial structure of the burgeoning state by counterfeiting the Continental dollar. The concept of the

economic manipulation of a state in a time of conflict stems from the assessment that absent the funds to pay and equip a fighting force that force degrades. The Revolutionary War example was remarkably difficult in that it required the forgery and covert distribution of currency into existing markets. The concept was to create rapid influx of fake currency to devalue the Continental dollar. The process of undermining the currency of an adversary in a globally connected world is simultaneously easier to forge and more difficult in to cause a devaluation. While the author knows of no examples of the cyber-enabled devaluation of a currency, there are examples of the theft of currency or the denial of access to currency to achieve strategic and tactical objectives. Moreover, there has been a significant change in how financial transactions are tracked and monitored globally to facilitate state objectives. This tracking and monitoring is a direct result of increased efficiency and connectivity. It is likely these tools, currently demonstrated in isolation against non-state actors, rogue states and targeted individuals within states could extend the effects of economic warfare in ways not yet conceived.[41] Moreover, beyond using the tools of a cybered world to establish constraints on certain actors, criminal organizations, terrorists, and states have demonstrated a willingness to leverage their hacking abilities to raid the financial resources of their perceived targets or adversaries with the intent of augmenting their financial capacity to engage in violence.

There are many examples of state and non-state actors attacking the financial integrity of other states within the international system. Most criminal exploits are undertaken for financial gain. The intent behind state-based attacks is less clear. Attacks by Iran on US banking infrastructure resulting in Department of Justice charges against Iranian nationals are indicative of the early stages of state attacks against financial infrastructures.[42] The North Korean attacks against South Korean financial infrastructure originally known as Dark Seoul, and now referred to as Operation Troy indicate sustained efforts at degrading or damaging financial infrastructure by leveraging multiple attack vectors.[43] These two cases are recent examples of a rapidly increasing number of cases of significant cyberattacks conducted against financial infrastructures in the US and other countries. Although there are active efforts to minimize the risk of cyberattacks against financial institutions through coordination and information sharing through organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). The threat landscape is large and daunting and will likely result in the continued convergence of cyber and financial warfare.[44]

Although the use of cyber means to engage in economic warfare is in and of itself not violent in the Clausewitzian sense of war in that death and destruction is not a direct result of the manipulation of financial infrastructures, it does provide an avenue to manipulate the resources the underpin the ability to achieve violence. The analysis within this section is extremely limited, yet the intent is to demonstrate that violence is not independent of

the systems which enable it. At the state level, the constraining of resources can degrade the effectiveness of militaries. Cyber means are now far more effective than bombing at disabling, dismantling and constraining the financial resources of state adversaries in most situations.

Hacking Humans

When the writers of *The Six Million Dollar Man* conceived of their show, they likely never considered the ability of states or criminals remotely hacking into to the bionic implants of their star to achieve ulterior goals and objectives. Science fiction is no longer fiction, doctors and patients are actively seeking solutions to a variety of common medical ailments through use of implanted medical devices (IMDs). During the period from 1993 to 2009 approximately 2.9 million US patients received pacemakers.[45] The features of modern pacemakers are extensive, including a variety of statistics and notifications on patient health, sleep modes, alerts for changes in cardiac function and more. Most modern pacemakers have some form of external connectivity that facilitates the collection of data from or programming of the device. Marc Goodman, a former law enforcement officer and author of *Future Crimes,* provides detailed anecdotes about the hacking of limbs, pacemakers, and other devices.[46] Goodman presents a scary future in which criminals hold individuals lives ransom with IMDs or take control of IMDs to achieve other nefarious ends. Like taking control of *The Six Million Dollar Man,* these hypothetical scenarios are chilling and achievable.

It is incumbent upon scholars and decision-makers to recognize the threats posed by the evolving digital world.

Numerous recent studies from academics as well as the National Institute of Standards and Technology have written detailed analyses of the vulnerabilities embedded within IMDs.[47] One of the most famous IMD hacking incidents occurred when Jerome Radcliffe presented at Black Hat, the world renowned hacker conference. His paper provided definitive evidence that it was possible to hack IMDs. He demonstrated the easy manipulation of various aspects of an insulin pump and provided relevant indications on the effects a hack would have on a human such as himself with an IMD.[48] The result would be death. Although there are no know incidents of hackers engaging in murder extortion through code, the demonstrated capability by Radcliffe and others provides perhaps the clearest direct impact of the manipulation of code for the achievement of violence. The threat posed to IMDs is so great that in a 60 Minutes interview in 2013, Former Vice President Dick Cheney indicated that when he had a pacemaker implanted in 2007, he had doctors disable its wireless capabilities to prevent a potential assassination.[49]

This section builds on other conventional applications of violence that are often more abstract and provides clear, demonstrated capabilities that achieve violence. There is little ambiguity that on an individual basis the ability to kill with code is a reality. While this violence is not universally applicable to entire populations as a bullet or a bomb, it serves to highlight the evolving threat landscape.

70 Ton Paperweights

A 2010 article in the *New York Times* on the number of computers in modern cars brought to the forefront perhaps one of the most effectual ways to accomplish violence through cyber means. The article notes that in 1977, the typical car had one basic computer for spark-plug timing, while today the average consumer vehicle will contain more than thirty computers and more than 100 million lines of code.[50] These computer systems control everything from ignition to breaks and steering and beyond. In 2014 at the Battelle Cyber Auto Challenge a 14-year-old built an electronic remote auto-communications device with $15 worth of Radio Shack parts in a single night.[51] The teen was able to turn on the vehicle and alter some of the non-safety related equipment. Six months later *Wired* columnist Andy Greenberg participated in a test with hackers that illustrated the remote hacking of a Jeep Cherokee while driving down the highway at seventy miles per hour.[52] The controls of the car were hijacked, and the transmission was switched off. The vehicle becomes a rolling paperweight. The hackers in Greenberg's test are not the only ones to demonstrate the vulnerability of cars to digital attacks. There have been multiple papers examining the concept, and even the National Highway Transportation Safety Administration has deemed it of significant concern to publish a 2015 white paper on Vehicle Cybersecurity.[53]

As a best-case scenario, a U.S. Air Force A-10 Thunderbolt II might be able to destroy half-a-dozen or more tanks in a single sortie if it has a near perfect flight. All the while the A-10 pilot must be conscious of threats from multiple other sources to include surface-to-air missiles, anti-aircraft weapons, and other air defense systems. At the same time, a distributed cyberattack against the various control systems that operate an Armored Brigade Combat Team (ABCT) comprised of more than 300 vehicles might be able to immobilize, commandeer the drive components or dramatically reduce the efficiency of onboard targeting computers, forcing soldiers to shift to manual sight. Within the US context as in many other nations, the code bases between the various platforms are similar if not identical. As tanks and other armored components become increasingly imbued with computers such as Russia's T-14 Armata, the potential effect of a cyberattack on one of land warfare's most impressive combat vehicles is astounding. While there is no way to fully eliminate the ability of an armored platform like an M1A2 Abrams from firing, the ability to damage its maneuverability or firing efficiency is a real possibility.

The problem is not confined to terrestrial components of war but extends to naval forces as well. In 2013, a team of researchers at the University of Texas at Austin were able to spoof GPS and divert an $80 million yacht. [54] Cyber vulnerabilities have led the U.S. Navy to reinstate programs focused on celestial navigation. [55] The systems that control the function of naval vessels, particularly on modern ships are increasingly digitized. Peter Singer and August Cole in their novel *Ghost Fleet* highlight the future of warfare in a fictional world where all the modern advances in computing are turned against their operators for military objectives. [56]

Violence in the form of a bomb can pale in comparison to the potential for violence achievable via code. Code, can take a seventy-ton weapon of war and make it into a $6.2 Million fixed artillery battery with manual sights. The reality of the violence of code to affect the tools of war should not be overstated. While there are very real demonstrated incidents of code affecting civilian vehicles and infrastructure, there are no publicly available sources indicating the same kinds of manipulation of associated with military equipment. While not demonstrated, the same underlying computer systems are present in both, and it stands to reason that if one is vulnerable, the other is also.

The Violence of Code

Code is not violent. It is logical representations input into computers. At its most basic code is the on and off of electrical impulses. These impulses direct a computer to engage in an action. Code can be used to create programs that provide insight into the universe, the human body, and efficiencies in transportation, finance, communications, and an almost infinite number of fields. The aggregate benefits of code are immense. Just as a gun can be used for sustenance and target practice it can also be used for killing. Where a gun is limited in its temporal and spatial relations for the achievement of violence, code can extend beyond these limitations and expose assets and individuals to risk in ways that are difficult to comprehend. While the present conceptualization of violence as the physical application of force intended to hurt, damage, or kill someone or something remains in many ways the standard definitional baseline for violence, it is limiting. The above discussion and cases are meant to illustrate that hacking, the unintended manipulation of code when directed towards a violent end can and does achieve violence. The end state of a violent hack has analogs that are well understood and studied by conventional IR theorists, law and policy makers. Just as the increase in weapons quantity and sophistication results in a security dilemma, so to can the development of hacking

The violence of hacking is something that must be addressed and incorporated into existing IR theory, legal and policy frameworks.

capabilities achieve many of the same objectives that a conventional weapon of war might achieve. Likewise, the pervasiveness of code can magnify the impact of non-armed force to include economic and political violence.

It is important not to overstate the threat of violence associated with hacking. The overstatement of the threat diminishes the real risks posed by those who would seek to leverage digital tools for the achievement of violence. At the same time, it is incumbent upon scholars and decision-makers to recognize the threats posed by the evolving digital world. As cars, aircraft, ships, trains, critical infrastructure and even human beings become increasingly digitized the number of potential vectors of violence will increase. Just as black powder increased the lethal range of a projectile, and nuclear weapons increased the destructive radius of conventional bombs, an increasingly pervasive substrate of cyberspace will expand the lethal potential of hacking for violent ends.

The semantic debates of law and international politics are important and help States determine the appropriate normative environment in which they exist. Michael Schmitt outlines a distinction between economic and political coercion and the use of armed force with seven criteria: severity of damage, the immediacy of the consequences, directness, invasiveness, measurability of damage, presumptive legitimacy, and responsibility.[57] These criteria fall outside of codified international law, yet serve as a foundation for future interpretations on the inclusion of non-traditional uses of armed force or state violence such as cyberattacks.

The value of a semantic debate should also not be overlooked. Scholarship by Thomas Rid, Jon Lindsay, Chris Demchak, Martin Libicki, and others serve as a forcing function for civilian and military decision-makers to ensure that the resultant policy frameworks and laws both internal to states and between states are built not on unfounded rhetoric but rather on a conscientious well-defined reality. There is little doubt that as the number of Internet-connected devices expands into the tens-of-billions and these devices seep into every aspect of our lives their ability to generate effects, including those which can result in physical violence will only increase. The violence of hacking is something that must be addressed and incorporated into existing IR theory, legal and policy frameworks. Just as nuclear weapons altered theory, law and policy, cyber weapons stand to do the same.

NOTES

1. "violence." *Merriam-Webster.com,* 2015, http://www.merriam-webster.com (March 7, 2015).

2. http://www.who.int/violenceprevention/approach/definition/en/.

3. Stephen Van Evera, Guide to Methods for Students of Political Science. Ithaca: Cornell University Press, 1997.

4. Colin Elman, and Miriam Fendius Elman, Progress in International Relations Theory: Appraising the Field. Cambridge: MIT Press, 2003.

5. William Gibson, *Neuromancer* London: Harper Voyager Publishers, 2013.

6. Hannah Arendt, *On Violence,* New York: Harcourt, Brace, Jovanovich, 1970.

7. "war." *Merriam-Webster.com,* http://www.merriam-webster.com, March 7, 2015.

8. See: Clausewitz, Carl von, Michael Howard, and Peter Paret, *On War,* Princeton, NJ: Princeton University Press, 1976, 43.

9. Kenneth N. Waltz, *Theory of International Politics.* Reading, Mass: Addison-Wesley Pub. Co 1979 102-104.

10. Robert Jervis, "Cooperation Under the Security Dilemma." *World Politics* 30 (2), Cambridge University Press, Trustees of Princeton University, 1978, 167–214.

11. Robert O. Keohane, and Joseph S Nye, Power and Interdependence: World Politics in Transition, Boston: Little, Brown, 1977.

12. Thomas C. Schelling, Harvard University, Center for International Affairs, 1966. *Arms and Influence.* New Haven: Yale University Press, 79.

13. Specifically here the intent is to indicate that the connection between the objective and the instrumental act of violence necessary to achieve that objective can and often does originate within a first order effect. However, violence is not constrained to first order effects.

14. Solomon W. Polachek, John Robst, and Yuan-Ching Chang, "Liberalism and Interdependence: Extending the Trade-Conflict Model," *Journal of Peace Research* 36 (4), SAGE Publications: 1999, 405–22.

15. A. A. Hoehling, and Army Times Publishing Company, *Vicksburg: 47 Days of Siege,* Englewood Cliffs, NJ, Prentice-Hall, 1969.

16. Serhii Plokhy, "Mapping the Great Famine," *Gis.Huri.Harvard.Edu.* Accessed February 28, 2016. http://gis.huri.harvard.edu/images/pdf/MappingGreatUkrainianFamine.pdf.

17. Thomas Rid, "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (November 2012): 7.

18. Carl von Clausewitz, Michael Howard, and Peter Paret, editors, *On War,* Princeton:Princeton University Press, 1976, 87.

19. "puslation." *Merriam-Webster.com,* http://www.merriam-webster.com,March 7, 2015.

20. See: JD Fearon, "Rationalist Explanations for War." *International Organization* 49 (3): 1995, 379–414.

21. Aaron F. Brantly, "Cyber Actions by State Actors: Motivation and Utility." *International Journal of Intelligence and CounterIntelligence* 27 (3): 2014, 465–84.

22. Carl von Clausewitz, Carl von, Michael Howard and Peter Paret editors, *On War,* Princeton: Princeton University Press, 1976, 87.

23. J. Stone, "Cyber War Will Take Place!." Journal of Strategic Studies 36 (1): 2013, 101–8.

24. Robert Anthony Pape, Bombing to Win: Air Power and Coercion in War. Ithaca: Cornell University Press, 1968.

25. "hack." *Merriam-Webster.com.* 2015. http://www.merriam-webster.com (March 7, 2015)

26. http://www.ustranscom.mil/cmd/aboutustc.cfm

27. Senate Armed Services Committee, Inquiry Into Cyber Intrusions Affecting U.S. Transportation Command Contractors, United States Senate, 113th Congress, S. REP. NO. 113-258, at (2014).

28. Ibid.

29. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39 (3): 2015, 7–47; Kramer, Franklin D, Stuart H Starr, and Larry K Wentz, 2009 "Cyberpower and National Security." Washington, D C; National Defense University Press: Center for Technology and National Security Policy; Potomac Books, William T. Hagestad, *1st Century Chinese Cyberwarfare.* Cambridgeshire [England]: IT Governance Pub, 2012.

30. International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention),* August 12, 1949, 75 UNTS 287, available at: http://www.refworld.org/docid/3ae6b36d2.html [accessed May 31, 2016].

NOTES

31. Michael N. Schmitt, Precision Attack and International Humanitarian Law, 87 INTERNATIONAL REVIEW OF THE RED CROSS, 2005 445, 446.

32. "Precision Air Warfare and the Law of Armed Conflict." *International Law Studies* 89: 2013, 694.

33. 14f00304 Documents https://d3gn0r3afghep.cloudfront.net/foia_files/14f00304-Documents.pdf from https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/#1212530-14f00304-documents, see 36.

34. Ibid., 57.

35. Ibid.,59-62

36. Ibid., 70-72.

37. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier ." Version 1.4 Symantec, 2011.

38. Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Crown Publishers, 2014.

39. Ibid.

40. Ben Baack, "Forging a Nation State: the Continental Congress and the Financing of the War of American Independence", *Economic History Review* 54 (4). Wiley-Blackwell: 2001, 639–56.

41. Exec. Order No. 13660, 31 C.F.R.(2014).; Juan Carlos Zarate, Juan Carlos, Treasury's War : the Unleashing of a New Era of Financial Warfare. New York: Public Affairs, 2013.

42. "Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities | USAO-SDNY | Department of Justice." *Justice.Gov,* 2016, Accessed June 7. https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

43. Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in South Korea." McAfee, 2013, http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf.

44. Juan C. Zarate, "The Cyber Financial Wars on the Horizon." Foundation for the Defense of Democracies, 2015. http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf.

45. Arnold J. Greenspon, Jasmine Patel, Edmund Lau, Jorge A. Ochoa, Daniel R. Daniel R. Frisch, Reginald T. Ho, Behzad B. Pavri, and Steven M. Kurtz, "Trends in permanent pacemaker implantation in the United States from 1993 to 2009: increasing complexity of patients and procedures," Cardiology Faculty Papers, 2012, Paper 18.

46. Marc Goodman, Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, New York: Doubleday, 2015.

47. Division, NIST Computer Security, and Electrosoft Services, Dr Sarbari Gupta, *Implantable Medical Devices - Cyber Risks and Mitigation Approaches,* 2012. http://csrc.nist.gov/news_events/cps-workshop/cps-workshop_abstract-1_gupta.pdf; Halperin, Daniel, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H Maisel, "Security and Privacy for Implantable Medical Devices." *Pervasive Computing,* January, 2008, 30–39; Tamara Denning, Alan Borning, Batya Friedman, Brian T Gill, Tadayoshi Kohno, and William H Maisel, "Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices," 2010,917–26.

48. Jerome Radcliffe, Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System, 2011, https://media.blackhat.com/bh-us-11/Radcliffe/ BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

49. http://www.cbsnews.com/news/dick-cheneys-heart/.

50. Jim Motavalli, "The Electronic Systems That Make Modern Cars Go (and Stop)." *The New York Times,* February 4, 2010.

51. Lucas Mearian, "With $15 in Radio Shack Parts, 14-Year-Old Hacks a Car." *Computer World.* February 20, 2015, http://www.computerworld.com/article/2886830/with-15-in-radio-shack-parts-14-year-old-hacks-a-car.html.

52. Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It." *Wired.com.* July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

53. Stephen Checkoway, Damon McCoy, Brian Kantor, David Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, and Franziska Roesner, "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In, 1–16.; 2015. NHTSA and Vehicle Cybersecurity | National Highway Traffic Safety Administration (NHTSA). Nhtsa.Gov, 2011.

NOTES

54. Erik Zumwalt, "Spoofing a Superyacht at Sea." *News.Utexas.Edu.* July 30, 2013. http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea.

55. "U.S. Navy Brings Back Navigation by the Stars for Officers." *NPR.org.* Accessed June 7, 2016, http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers.

56. P.W. Singer and August Cole, *Ghost Fleet: a Novel of the Next World War.* Boston: Houghton Mifflin Harcourt, 2015.

57. Michael N. Schmitt, "The 'Use of Force' in Cyberspace: a Reply to Dr Ziolkowski," 2012, 1–7.