Ryan Carpenter

POLS 370.01

Cyberwar, Robots, & Conflict

Cyber Proliferation

"The cyber revolution is the revolution of our time; The rapid expansion of cyberspace in society brings both promise and peril" (Kello, 2017). As humanity has progressed, we have witnessed revolutionary advancements in technology such as the industrial revolution of the 19th century, the nuclear revolution of the 1940s and now the cyber and technology revolution of the 21st century. During the nuclear revolution, humanity witnessed the development of technology able to destroy entire cities with a single blow. The modern-day cyber revolution has yet to truly deploy acts of carnage in the form of cyberweapons, but as this revolution grows at an uncontrolled rate through societies new dependency on technology and automation. Humanity has once again stretched the traditional battlefields of conflict into a new-found realm of desired offensive and defensive superiority within the virtual world. Through the abilities of proliferation, cyber systems manipulation, and the requirement for new oversight; cyberwarfare will become and remain one of the most prominent challenge to democratic freedom and state sovereignty that the world has ever seen.

Formulated as a piece of knowledge and intelligence-oriented tactic, Cyberwarfare has continued to grow to greater lengths with uncapped payload capabilities. These often malicious tactics first appeared in the early 2000s through the development of "worm" technology. Since the early 2000 operations, cyberweapons have grown in sophistication and capability. It wasn't until 2010 with the deployment of the Stuxnet virus that skeptics and politicians opened their eyes to the capabilities of cyberattacks. Stuxnet was a complex piece of malware designed to interfere with Siemens' industrial control systems. It was discovered in Iran and Indonesia, leading to speculation that it could be a government cyberweapon aimed at Iranian nuclear programs. This operation was considered successful in destroying nearly a fifth of Iran's nuclear centrifuges while also opening a seeming Pandora's box in the art of cyberweapon development. In March and May of 2014, the world witnessed two Russian coordinated attacks against Ukraine and their election commission. The March attack was used in unison with combat operations, once again a first for the world. This DDoS attack was aimed at disrupting the Ukrainian internet while armed Russian rebels seized control over Crimea. The second of this dual-pronged offensive came three days before Ukraine's presidential election. Russian based hacking groups successfully took down the Ukrainian election commission and their back up system in an attempt to create chaos within the public while aiding the pro-Russian candidate. Then in 2017, The WannaCry ransomware crypto worm was anonymously deployed, affecting more than 2000,000 computers across 150 countries. More recently in June of 2017, the world was witness to weaponized ransomware. The NotPetya malware disguised as ransomware was deployed in Ukraine to destroy files. This attack then went uncontained and rapidly spread worldwide. Today, there still is not an exact count on the damages done by this attack, but speculation produced estimates over 10 Billion USD.

Lucas Kello, a senior researcher and lecturer on International relations at Oxford University and author of "The Virtual Weapon and International order," divides the development of cyber weapons into two categories, the ‘high wall' of powerful cyberweapons more tailored towards hostilities between nation-states and the ‘shallow moats' of generalized cyberweapons used more regularly by small actors such as terrorists organizations, thief's, and extremist. "High wall' operations can create catastrophic effects on a victim nation but are incredibly difficult to finance and develop as they are expensive, time-consuming, and amazingly sophisticated. This level of creation consists of customized code with a vertical leap of development and will often result in an innovative cyber weapon. "Shallow moat" operations, on the other hand, are relatively inexpensive and consist of more reverse engineering and code emulation which is much less time consuming but also restrictive in capabilities. Both forms can result in an incredible amount of sabotage against a nation state or powerful corporation, take the Sony Pictures hack of Nov 24th, 2014 for example.

The added twist that cyberweapons bring to the table, unlike kinetic weapons, as Kello writes "perforation denotes the acquisition of a preexisting or similar weapon by an actor other than its creator" (Kello, 2017, 178). What's important to realize in comparison to more recognizable kinetic weapons, the "virtual weapon is essentially massless. It does not occupy physical space. It is a knowledge-intensive capability" (Kello, 2017, 178). The notion of cyber proliferation varies upon interpretation as there is no clear right or wrong answer. Proliferation brings together the unpredictable capabilities and combines them with the ever-evolving landscape of baseline code which powers a weapon personalized by knowledge. Admiral Michael Mullen, Chairman of the U.S. Joint Chiefs of Staff, once commented "were going to have a catastrophic [cyber] event. Some of these tools already being built are going to leak or be sold or be given up to a group that wants to change the world order and were incredibly vulnerable" (Kello, 2017, 175).

Within cyberwarfare proliferation, Kello believes that there are two different forms: line replication and design emulation (Kello, 2017,178). A "high wall" structured weapon like Stuxnet is often produced using the method of design emulation. Design emulation is much costlier and a time-consuming process as it involves the redevelopment of source code. This, in turn, does provide more flexibility in capability customization and also creates the possibility of vertical or horizontal evolution. Vertical and horizontal evolution is the reason this art of cyberwarfare is increasingly unpredictable and untamable. "High wall" operations, with their knowledge-intensive process, have a slower rate of proliferation and expensive budgets so they are often rare; rare and dangerous. Generalized cyberweapons have a much greater potential for success as line replication is not only cheaper but less intricate and complicated. The lesser demands of generalized "shallow moat" style of attacks often fall into the hands of non-state players like scammers, extremists and terrorists; whereas "High wall" operations are likely state-organized and deployed strategically. When looking at the cyberwarfare landscape you can see that with every offensive, there is a very real risk of code evolution and the creation of malware or ransomware worse than originally developed and deployed.

Through the risk and constant evolution of this cyber environment, modern deterrence for this new virtual threat has become a paramount concern for state powers. As we observe an increasing frequency of these cyberattacks, Kello credits this to a political and worldly environment that has not kept pace with the evolution of the cyber battlegrounds. Modern Deterrence theory emerged out of the nuclear revolution, to which the cyber revolution is justly compared to. This theory revolves around the principals of denial and punishment and cyberwarfare spoils the logic of each in its respects. "Denial deterrence works by reducing the effectiveness of the adversary's weapons" (Kello, 2017, 207). Within the nuclear realm, theorists had determined there were two ways of achieving this goal. One was the development of kinetic defenses able to shoot a nuclear weapon out of the sky, and the second involved a mutual reduction of strategic forces. Neither technique is easily achieved against cyberattacks due to their unpredictability both in timing, stealth, capabilities, and not to mention the knowledge-based, non-tangible aspects of these virtual weapons. The accountability aspect of de-weaponizing would be impossible to calculate. Currently, we can observe state powers exploring the relationships between "the desire to deter major cyberattacks with the threat of severe penalties and the interest in controlling crisis when deterrence fails" (Kello, 2017, 269).

Kello offers two ideas that I support and believe is a start in the right direction towards an inevitable future. First, the idea of "punctuated deterrence" and secondly, the understanding that pure denial of cyber operations is seemingly unfeasible. Attempting to try and simply deny these acts and stop them all together is insurmountable and probably unattainable. Therefore, this new theory of cyberwarfare deterrence should be focused around the development of a measurable scale revolving around the calculation of intensity, timescale, and range of harm for every attack experienced. By tracking and using this evidence, world leaders will be able to determine true acts of aggression from nation-states that may warrant retaliation in the form of politics or hostilities. Kello writes "the goal is not to prevent all attacks, but to reduce their cumulative effects to a tolerable level" (Kello 2017, 269). I also believe that there should be an aspect of research and development involved in receiving generalized small level cyberattacks. The more the private and government cyber sectors can analyze malware, the more you can prepare defensively while producing and deploying offensively.

Cyberwarfare is the future of state and non-state meddling and will forever be one of the greatest tests for democratic freedom and state sovereignty. Despite the skeptic's opinions, "cyberattacks can cause enormous harm to national security even if its effects are nonphysical" (Kello 2017, 68) and should be of the utmost concern of nation-states as they continue to go unmonitored and unregulated. Harvard professor Jonathan Zittrain once said, "Cyberattack need not result in physical destruction to pose a danger to society." "It may not be a bomb coming down out middle chimney of our house, but it could be something that greatly affects our way of life" (Kello, 2017, 75). I firmly agree with professor Zittrain's opinion that one day we may experience the effects of a large scale cyberattack with the intent of hurting civilians. As Kello states "Officials at the U.S. Department of Homeland Security, for instance, have identified sixty-five facilities in the United States against which a single cyberattack could cause ‘catastrophic harm,' which they defined as ‘causing or having the likelihood to cause $50 billion in economic damages, 2,500 fatalities, or a severe degradation of our national security" (Kello, 2017, 74).

Kello's opinionated stance on punctuated deterrence begins to lay the groundwork for possible method to control cyber warfare at an international level. But as the cyber capabilities continue to grow, there is a mounting necessity for cyber alliances and limitations imposed by an international committee. Through the creation of an international committee, a standard can be imposed to reinforce a scale of appropriate punishments for cyberattacks based around the premises of punctuated deterrence. By controlling and implementing an agreed-upon limit, a secondary effect of controlling the state v. state styles of cyber conflict, which are more powerful and intent driven, may be moderately reduced. Granted, this is all a very utopian way of thinking. But if a higher level of awareness and international policy are not met, cyber-meddling will only continue to escalate progressively, up to the point until humanity finds itself amidst a near cyber Armageddon. Unfortunately, with the unpredictable and untamable nature of the cyber world, without any sort of understanding and regulation, this new way of inflicting damages to one's enemy is going to become something that humanity was not prepared for at the end of the day.