Keynote presentation given at the International Conference on Cyber-Warfare and Security, 28 February – 1 March 2019, STIAS, Stellenbosch, South Africa

The Role of Cyber in National and Global Human Security

Edward L Mienie, Edward.Mienie@ung.edu

Department of Political Science and International Affairs

University of North Georgia, USA

Abstract

Cyber is deeply enmeshed and interwoven across national security, as evidenced by its inclusion in the national security policies of a growing number of OECD countries. But it is the impact of cyber across the other components of national and human security that remains to be sufficiently addressed at the national policy level, or in international standards of behavior with respect to cyber warfare and hybrid conflict. In addition to standing on its own as a national security concern, cybersecurity impacts economic and trade security, ecological/environmental and biosecurity, energy and critical infrastructure security, food security, transportation and public health, as well as communications, physical and even political security. Nation states, criminal organizations, terrorists, insurgencies, private military contractors, corporations – and individuals – play a role in national cybersecurity threats and mitigation. This paper examines the role of threats from cyber warfare and hybrid conflict across human security from a national and global perspective, makes a few predictions about the near future of cyberwarfare, and provides recommendations for consideration by large and small nations with respect to preparing for cyberwarfare and ongoing hybrid conflict.

The Advent of Cyber Warfare

In 1947 the third industrial revolution was introduced with the invention of the transistor from which flowed massive technological changes that transformed societies and economies in the world. This resulted in governments, military and civilian organizations investing heavily in computer systems, making computers an essential part of normal operations during the 1950s and 1960s. Then in the 1980s, digital technology proliferated and computers invaded all aspects of life in developed nations. We see this with the proliferation of the Internet and the smart electricity grid, industrial robots, graphics for entertainment video games, automated teller cash machines in banks and in 1995 the world wide web expanded across the globe and became widely available.

The beginning of the 21st century introduced the smartphone, which quickly became commonplace. In 2017 we had 5 billion smartphone users and approximately 4.2 billion users accessed the internet while 85% of the infrastructure of the Internet is privately owned. The world became interconnected using smartphones, tablets, and computer-based devices for social networking. By 2015, cloud computing was ubiquitous, data could be uploaded in real time, and we saw tablet computers and smartphone use exceed personal computer use. During these past two decades especially, as governments and defense manufacturers realized the potential for smart weapons, a new generation of technological military systems and missiles were developed.

In 1946 the US Army Ordinance Corps financed and developed the world's first true reprogrammable computer. In 1952, President Harry Truman established the National Security Agency who in turn became a major investor in and customer of primitive computers and by 1985 NSA merged with the National Computer Security Center to house the world's single largest group of supercomputers in the world. In the 1960s, Cray Data Corporation first introduced supercomputers and could process 33 quadrillion floating-point operations per

second. At a price tag of $500,000 apiece, this placed Cray in hands of well-funded governments and handful of very big banks and corporations in the world. Today, NSA's latest facility at Fort Meade houses one of three High Performance Computing Centers each with their own 150-megawatt power substation providing 60 megawatts of electricity. Each center comes at a price tag of $3.2 Billion. The British NSA equivalent, GCHQ, has remained in step with the digital revolution, as have the other members of the UN Security Council. Digital intelligence is very high on the Chinese list of national priorities.

With real-time digital intelligence now available, the Intelligence Community (IC) has accepted that it is here to stay. There is a school of thought that the traditional intelligence cycle approach (Tasking, Processing, Evaluation, and Dissemination) is too slow. Digital intelligence is revolutionizing the way intelligence does business. The IC now needs algorithms and applications to work on data and provide recommendations in order to keep pace with open-source media.

In 2009, the US Cyber Command was established to operate in the digital space and recruitment and retention of a technically qualified cyber force has become a challenge. There is talk of changing (not lowering) recruiting standards in an effort to recruit geeks and nerds as never before. The creation of a separate cyber corps has become a struggle among military bureaucracies worldwide because of interagency competition.

The digital revolution has exposed the vulnerabilities of governments and these have to be addressed by digital means, otherwise known as cyberwar. For the past century, the frontlines of war have moved closer to the Western households, as war is no longer something that happens on a far-away battlefield. The illusion of living in the safety of our own homes is slowly being

eroded, as we increasingly become victims of cyber breaches, malware attacks, denial of service (makes a machine or network unavailable to its intended users), and the likes.

When is a War Not a War?

Cyberwar is a threat to society everywhere. In 1988, Robert Morris became the first person to be convicted under the US Computer Fraud and Abuse Act. His act became known as the "MorrisWorm", which used weaknesses in the UNIX system and spread around a number of computers. This worm slowed down computers to the point of being unusable. It is understood that today he is working as a professor at MIT!

In 1994, a Russian called Vladimir Levin used a laptop in London to access the Citibank network. He obtained a list of customer codes and passwords and passed them on to friends. He used wire transfers to steal $3.7 million and set up accounts in Finland, US, Netherlands, Germany, and Israel. His accomplices were eventually arrested and they implicated Levin who was detained by the British police in 1995. Citibank recovered all but $400k of the eventual $10.7 million stolen.

Computer hacking has become a genuine international threat and is becoming more widespread and dangerous. Classic security targets of espionage, sabotage, and to a lesser extent subversion are in the sights of hackers. Cyber-attacks are hard to pin on any adversary at the time of the attack, but intelligence agencies are becoming significantly more skilled at attribution, especially among highly skilled peer nations and known non-state groups. It used to be that the most damaging of cyber-attacks were Denial of Service or DoS attacks, but we are now seeing

large-scale ransomware attacks, targeting banks, credit card companies and local government. The city of Atlanta, the ninth largest US metropolitan city, was crippled by a ransomware attack in March 2018 that shut down city government functions including courts, police records, and municipal water payment systems. Several years' worth of video footage captured by the city's police cars was lost and unable to be recovered (Deere, 2018). Over $17 Million in direct costs were disclosed, in addition to the reputation damage, lost productivity, and other so-called soft costs (Spitzer, 2018). Notably, the ransomware was attributed to two specific Iranian civilians, who were named by the FBI and indicted in November 2018.

Other targets of opportunity include infrastructure such as power plants, water systems, fuel depots, communications, and transportation. Satellites are particularly vulnerable as this could compromise military systems such as control and command. Nuclear release codes could also be vulnerable.

In 2009, there were reports of Russia and Chinese attempts to infiltrate the US electrical grid. They left behind software programs that could be used to disrupt the system. As recently as November 2018, US intelligence officials noted that Russian hackers were still actively probing US power grid targets for vulnerabilities (Newman, 2018). National and municipal utility companies around the globe are advised to be on high alert, both for direct attacks like those noted above, and for "fallout" effects and collateral damage that might occur against uninvolved nations, when two or more larger powers conceivably launch targeted cyberattacks against commonly used systems and equipment.

From an intelligence point of view, the worst nightmare is not knowing who the enemy is while the attack is happening. The espionage danger is real by using illegal exploitation methods on the internet to obtain secret information for political, military, or economic advantage. There

is a real danger in intercepting and even modifying classified information from the other side of the world not knowing who it is or whether it is genuine or not!

In 1999, the US accidently discovered someone trying to access the systems at the Pentagon, NASA, the US Department of Energy, private universities, and research labs. The US traced this back to Russia but Russia denied this and the sponsor is unknown. The so-called "Titan Rain" attack in 2013 on Redstone Arsenal in Huntsville, Alabama, was most likely perpetrated by the Chinese but the precise nature is not known until today, e.g. is it state-sponsored espionage, corporate espionage, random hacker attacks? The real identities were masked by proxy sites, "zombie computers" which infected spyware/viruses into the computer systems. The base is used as the Centre for the US Army's missile and rocket programs.

In 2007, cyber war became a reality for Estonia when Denial of service attacks disabled parliament, banks, newspapers, and broadcasters' computer networks. The Russians called the accusations unfounded and there was no evidence of their complicity. However, the head of the Russian military forecasting center later confirmed their ability to conduct such an attack. This is yet another example that poses a problem from the US IC by not knowing for sure the perpetrator of the attack.

The first major cyber-physical attack on critical industrial infrastructure occurred in 2009 when a very sophisticated attack was launched on Iran's centrifuges that came from a memory stick flash-drive through a Microsoft Windows operating system to the Siemens Step7 software that controlled the centrifuges. This was a malicious computer worm called "Stuxnet." No-one at the time knew where it had come from originally or who the intended victims were meant to be. Siemens claimed industrial espionage had been perpetrated against their business, while Iran claimed that their nuclear program had been sabotaged. Which was it? A combination of the

two? How do we decide to retaliate? Against whom? By what means? And to what extent? While both the US and Israel are alleged as the possible sources of this cyber-physical weapon, neither has publicly acknowledged responsibility. Although, it is believed that at General Ashkenazi's retirement from the Israeli Defense Force farewell reception, he referenced "Stuxnet" as one of his operational successes. While most of the collateral damage caused by Stuxnet was reported to be minimal, it affected systems in Germany (where the Siemens controllers originated) and elsewhere in smaller nations that were not involved in the dispute between Iran and its adversary or adversaries.

In 2014, the second known successful cyberphysical attack was revealed, this time apparently targeting a steel mill in Germany (Zetter, 2015). The software disrupted a blast furnace control system so that the furnace could not be properly shut down, causing massive damage to the facility. Previously, in 2013, seven members of Iran's Islamic Revolutionary Guards Corps allegedly took control of a flood-control dam 25 miles north of New York City through a cellular network modem, but they were unable to release water only because the sluice gate had been disconnected for maintenance at the time of the attack (Thompson, 2016). The FBI used its "name and shame" tactic both to limit travel options for the seven individuals claimed to be involved, and to demonstrate that the US was getting better at attribution, even though it took over two years to bring the indictment. The attackers were also targeting banks, the New York Stock Exchange, and telecommunications giant AT&T.

Several smaller cyberphysical effects were achieved through ransomware similar to that used in the attack on the city of Atlanta, though. Especially in the cases of hospitals, such as the Hollywood Presbyterian Medical Center ransomware attack in February 2016 (Winton, 2016). While the hospital paid the $17,000 bitcoin ransom and recovered control of its computers, in the

week and a half of the shutdown caused by the ransomware, several patients were sent to other area hospitals, although no cases of direct injury to patients were noted.

In addition to public health facilities, themselves, individual medical devices, such as pacemakers and insulin pumps, have been found to have major vulnerabilities that could conceivably cause deaths from targeted cyber-physical attacks against these devices (Hern, 2018). While no patient deaths have been reported to date as a result of hacking, there have been recalls affecting as many as half a million devices in a single case (Hern, 2017), affecting both private medical device manufacturers and hundreds of thousands of patients.

Perhaps the largest cyberphysical attacks, though, were the two separate attacks on Ukraine's power grid in December 2015 and December 2016, which shut down power to hundreds of thousands of customers in the cold of winter (Greenberg, 2017). Each attack lasted only a few hours, the length of time it took engineers to scramble to physical substations to engage manual override switches. But they demonstrated the power and precision of the alleged Russian military cyber war machine, with the second attack fully automated and striking at precisely midnight on Saturday. The attacks contributed to the destabilization surrounding the annexation of Crimea and several clashes between Russian and Ukrainian forces in the Donetsk and Luhanks regions of Ukraine. This time, attribution was relatively swift, but the smaller Ukraine was not able to retaliate in kind against its much more cyber-capable adversary.

In 2011, Richard Clarke, the White House counterterrorism chief warned that the US had already lost the cyber war even before it started. He pointed out that Russia, China, and NK already recruited legions of hackers, while Iran boasts of having the world's largest cyber army. He warned that because we are so utterly dependent on electronics, the West could be brought to its knees within fifteen minutes. Since then, cyber-attacks have become regular features of an

undeclared war. The Chinese People's Liberation Army is known to be hacking into major US and European corporations going after intellectual property and targets include IT, electronics, software, defense, aerospace, biomedical and pharmaceutical breakthroughs, energy, finance, banks, and agriculture. In 2012, a major Russian IT security company called "Kaspersky" identified a cyber-attack called "Red October" that had been operating since 2007 and it used Word and Excel to gather information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.

MI5 and the Director General of GCHQ has expressed concern about cyber-attacks and how that may cause significant damage to their reputations and revenue. US Cyber Command has to decide daily whether they are being confronted by criminal activity or breaches of national security. Into which category does commercial espionage and theft of intellectual property fall? In 2014, after Sony Pictures produced a low budget movie poking fun at Kim Jong-Un. He launched 6,000 hackers against Sony, which inflicted a cost on Sony of $100M. The FBI claimed to have conclusive evidence that it was the NK government behind it. President Obama called them out and retaliated with a controlled cyber strike against NK's weak internet. Was this a case of cyber terrorism, cyber war, or cybercrime? NK has denied their complicity and has demanded an apology. It should be noted that not everyone is in agreement with the FBI's conclusion that the attack was indeed perpetrated by NK. The detractors claim that the attack was too sophisticated and that it was more than likely an insider job. This is a great example of the difficulty a cyber-attack poses to the IC by not knowing for sure who the enemy is and yet a counter-offensive was launched. This cannot bode well as an example of possibly misidentifying the attacker and launching an attack on the wrong target. We are stuck with the underlying difficulty of identifying the real cyber aggressor. We should keep in mind that weak retaliation

emboldens others and the bad actor can maximize the threshold-level event to suit their aims and objectives. This could make cyberwarfare the ultimate asymmetric war and has changed the landscape of cyber conflict.

Legislation would have to be passed by Congress for there to be intelligence sharing between the IC and the private sector. The Snowden case warned about this. The US has much more to lose than any other nation because it has more research and development than anywhere else in the world. There is a definite cyber-threat to this type of intelligence sharing. Sixty percent of known cyber-attacks are against commercial targets. Cyber-attacks is the 21st century preferred form of international trade theft. The threat is growing exponentially and in 2015 it increased by more than 600% over a three-year period. Attempts to breach security in the energy, oil, and gas sectors increased to just under 400 percent. Questions that we are facing are how much security is enough? Should it be run internally or outsourced? How much should be spent? What tools and people are most effective?

As the Chinese state and its economy are intertwined, illicit intelligence gathering raises to the level of national security interests. The pressure of economic sanctions against Russia due to their actions in the Ukraine has resulted in an increase in cyber-attacks against the West. The cyber-attack growth from 2009 to 2015 increased from 3.9 million incidents to more than 50 million. We have observed that international agreements to limit such behavior are ineffective. Russia and China strongly deny accusations of intellectual property theft or cyber espionage. However, in light of NSA activities as revealed by the 2013 Edward Snowden saga that the US spied on Germany and Brazil, China and Russia have become emboldened to accuse the US of obvious hypocrisy.

It is no longer a secret that the US, Russia, China, Israel, and NK are engaged in a ruthless, secret and potentially dangerous cyber struggle. By 2016, the Pentagon's IT and cyber programs increased six fold in spending from $13.3 million in 2015 to $84 million in 2016. To further underscore the resolve of the US Government to do everything possible to mitigate the threat of cyber war, the CIA announced in 2015 their first new Directorate in fifty years, namely the Directorate for Digital Innovation. The problem we face is that no-one knows exactly what the real threat is and because of that there is a strong temptation to throw taxpayers' money at some ill-defined enemy. As an alternative to conventional warfare, cyber war is a new, ill-defined form of warfare with intelligence at its cutting edge. As the threat of hybrid warfare is increasingly growing to replace conventional warfare, a cyber-attack has become the main disabling weapon.

And especially in smaller nations, we must not only protect ourselves from direct cyber threats from both terrorist groups and other nation-states, but from the potential collateral damage resulting from larger powers' use of cyberweapons both in warfare and in so-called hybrid conflict short of war.

The era of cyber war has introduced weapons of mass disruption as opposed to conventional war's weapons of mass destruction. Weapons of mass disruption are temporary, such as the "Stuxnet" example, specialized, ongoing, secret, and a crime and a nuisance. On the other hand, weapons of mass destruction can cause huge casualties such as the case of Hiroshima and Nagasaki, are indiscriminate, transparent, and fall into the category of warfare and are strategic. We should also be mindful that there is no single accepted definition of "cyber" and analysts and even states talk past each other when using the term. Some people regard cyber as actions through the internet. For others it involves information warfare. Not having a universal

understanding of the term makes understanding and responding to different threats very complicated. Perhaps it is best to think of cyber as comprising a set of tools and the question then is not which cyber technologies can do something specific, but rather how the changed context changes the way we understand and interact with the world (Dr. Andrew Futter, 2018).

What does the cyber weapon of the future look like? While no one can say, or will disclose, with certainty, here are a few of the considerations that nations large and small should keep in mind to protect national and human security in this period of cyber proliferation and cyber escalation. Human security concerns such as attacks on power/water supply, medical systems, or other physical systems could endanger public health

First, we have already seen most of the individual weapons. What will be different in an all-out cyber war is the massive aggregation of cyber weapons in a coordinated barrage of attacks: ransomware launched broadly against hospitals, public safety, banks, transportation and logistics firms, and local governments; highly targeted power and water disruptions in major cities; information operations and disinformation campaigns aimed at social media and traditional news outlets; and massive denial of service attacks against stock markets and major telecommunications providers. Information operations and info warfare can achieve scale and speed never before possible (did fake postings on Facebook impact US election?). And imagine the impact of all that going on, while simultaneously experiencing traditional kinetic attacks against key military and political targets on the ground from artillery, missiles and good-old-fashioned bombs. Future warfare is not just cyber war, but cyber *plus* war. It is not War 2.0 or 3.0, but War to the second or third power, *exponentially* more devastating than traditional or even nuclear weapons alone.

Second, social engineering and traditional human intelligence operations will continue to *grow* in importance in cyber warfare. Releasing targeted weapons over the Internet is complicated by considerations of collateral damage, as was the case in Stuxnet and several ransomware attacks, and it increases the risk of detection and neutralization by third parties. Human intelligence operatives will continue to be able to deliver portable USB drives and other physical electronic devices, combined with ever-evolving remote and local social engineering attacks, to gain access to even air-gapped, non-networked systems like those in sensitive government, military, and public utility company operations. Cyber operators will not replace intelligence operatives, as some have envisioned; rather, they will rely even more heavily upon their human intel colleagues, both to bring sensitive information to the table, and to deliver targeted electronic payloads where signals, wires, and fiber optic cables may not reach.

Third, cyber defense will evolve and morph almost as rapidly as the shifting cyber landscape. Vigilant cyber hygiene and aggressive patching and updating of systems is not enough. We must also expand and accelerate cyber operations training for professionals in military, government, *and* corporations. Currently, there is a global skills gap of over 1 million unfilled cyber jobs and we cannot just throw money at cyber if there is no workforce to carry out the mission.

We must become orders of magnitude better both at cyber threat hunting and at sharing information on likely cyber attacks and vulnerabilities between national agencies and private industry. The US has begun efforts toward this end, but it may be hindered by its size; this is an area that smaller nations could potentially do better than their traditionally more powerful peers.

Finally, cyber warfare will continue to be exacerbated and to some extent obscured by traditional cybercrime and espionage, which we can only characterize with the word “more”.

More denial of service attacks, more Internet of Things attacks, more ransomware and crypto attacks, more targeted attacks against specific infrastructure and devices, and more information warfare. More disruption, more annoyance, more danger to our economies, our borders and biosecurity, our food, energy and natural resources, our transportation and communication, and even our public health, physical and political security.

In conclusion, cyber is deeply enmeshed and interwoven across national security concerns. In the interests of more cyber threat awareness, we propose that tabletop exercises and cyber simulations for political leaders, armed forces, police, and critical infrastructure personnel down to the local government level be conducted regularly. Awareness training for civil and municipal government employees should be the norm and not the exception. Telecom companies and device manufacturers can assist in prevention of malware, phishing, and network-borne attacks by being proactive in our combined efforts to mitigate those attacks and to share information with government agencies in a more concerted and immediate manner. Moreover, technology and cyber education in schools should become part of the core curriculum. The moment our fingers touch a keyboard or touchscreen, or the moment we use our voices to interact with the technology listening in our cars, homes or smartphones, irrespective of our educational discipline, we are exposed and vulnerable to a cyber-attack. Individual responsibility can mitigate national cybersecurity threats collectively, but we must make a collective effort to develop a new generation of cyber heroes, cyber guardians, and cyber professionals. An uneducated populace is a luxury developed nations can no longer afford. It is our sincerest hope that discussion and acknowledgment of the scope of future war, and that public, academic conferences like this one can spark the kinds of national policy debates that can energize our collective will to prepare for the next generation of cyber warfare that is already at our doorstep,

that we have already seen in part, but that has the potential to forever change our future and our children's future.

[Thank you for your time and attention, and I look forward to taking your questions.]

Deer, S. 2018. https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/

Greenberg, A. 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/

Hern, A. 2017. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

Hern, A. 2018. https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic

Newman, L.H. 2018. https://www.wired.com/story/russian-hackers-us-power-grid-attacks/

Spitzer, J. 2018. https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-may-cost-the-city-17m.html

Thompson, M. 2016. http://time.com/4270728/iran-cyber-attack-dam-fbi/

Winton, R. 2016. https://www.wired.com/story/russian-hackers-attack-ukraine/

Zetter, K. 2015. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/