PAMUN XVII RESEARCH REPORT— QUESTION OF STATE SPONSORED CYBER TERRORISM

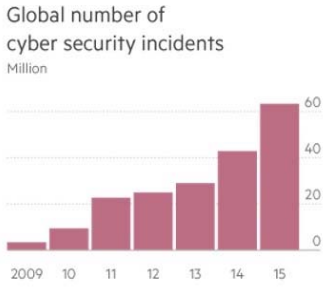
Introduction of Topic

In 1965, after careful observation of emerging trends, Gordon Moore predicted that the power of computing would double every 18 months. Also known as “Moore’s Law”, this theory has set the exponential momentum of our modern digital revolution while also alarming governments of vulnerabilities the phenomena brings.

As a result of increasing interconnectivity, critical infrastructures are now exposed to a growing number and a wider variety of threats that raise new security concerns. In just 15 years, the number of individuals using the Internet has soared from an estimated 16 million in 1995 to more than 1 billion in 2010. Meanwhile, government reliance on computer systems and networks has increased exponentially.

Cyberspace has become like a large city: it allows for crossing paths with dangerous individuals. These include State actors whose full time jobs are to destabilize nations by hacking and interfering with the very systems and sensitive information that their infrastructure, defense networks, and industries rely on.

State-sponsored attacks have grown since 2009. Incidents increased between the years 2009 and 2015 by 38% in 2015 compared to 2014.



Increasing cyber attacks between the years 2009 and 2015

Over 20 countries have announced their intent to launch or strengthen offensive cyber capabilities to keep the upper hand in the virtual war. The result is a burgeoning digital arms race that presents a major threat to all nations.

Although we were once separated from destructive ideologies and dictators by the physical buffers of oceans, we now co-exist in a cyber world with no geographic boundaries and few capabilities to enforce law.

Our modern economies have become increasingly inter-connected yet our abilities to prevent cyber terrorism haven’t kept to pace. Global disruption is just a click away.

Definition of Key Terms

Terrorism

Although the United Nations has not yet decided on a definition of the term, the Security Council in 2004 agreed to defining a 'terrorist act' as: "a serious criminal violence intended to provoke a state of terror, intimidate a population or compel a government or organization."

Cyber terrorism

Cyber terrorism is the politically motivated use of computers and information technology to cause severe disruption in society. It encompasses cyber attacks, where immediate damage is caused, and cyber espionage, which can provide the necessary information to conduct a successful cyber attack.

Cyber attack

A cyberattack is the breaching of a computer system with the intent of stealing property or financial resources, disabling or wiping out files, or causing any other damage to a network. Countries conduct cyber-attacks to achieve strategic, economic, diplomatic, or military advantages by attacking military, government, or civil computer infrastructures. Cyber threats are of serious concern for governmental leaders. Former President Barack Obama called such a menace: "one of the most serious economic and national security challenges we face as a nation."

Critical infrastructures

Critical infrastructures are those whose physical or online systems are essential to the operations of the economy and government. They include but are not limited to telecommunications, transportation, defense, emergency services, food distribution, air and maritime support, banking and financial services, as well as the crucial information that interconnect and affect the operations. Destructing critical infrastructures is one of the focal goals of cyber terrorists.

Vital infrastructure examples

Malware

Malware, or "malicious software", is software intended to infiltrate, damage and disable computers or other technological devices.

Firewall

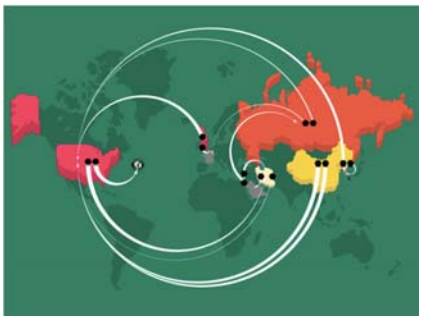
A firewall is a network security system that acts as a barrier to control incoming and outgoing network traffic. Cyber terrorists often break through firewalls to achieve their hacks.

State-sponsored actor

A State-sponsored actor is one who operates with the support and funds of the state. A nation-state actor, unlike a simple cyber criminal, has immense backing when it comes to capital and time. Attacks originating from foreign governments are often deployed in exactitude as the actors have the immense financial endorsement and advanced tools of the State.

Background Information

Centuries ago, monarchs recruited mercenaries and supplied them with arms to ambush countries oceans away and gain riches. Today, instead of being given weapons, State-sponsored actors are afforded extensive resources and technology to accomplish a new 21st century mission: infiltrating networks. Once it was recognized that targeting digital systems was much simpler than sending soldiers into the battlefield, nation-states began developing their cyber technologies. At the same time, national security agencies have been developing cyber defense capabilities to protect their nations.



Cyber attacks conducted between the years 2010-2014

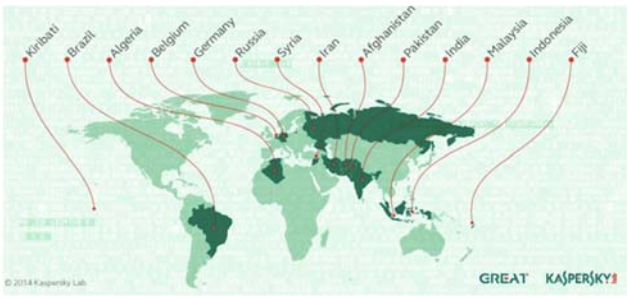
Main cyber terrorist attacks

'Stuxnet' (2010)

The 'Stuxnet' worm remains one of the most famous cyber weapons as it was the first to severely shatter the security industry when discovered in 2010. The highly advanced malware targeted control systems of centrifuges in Iran's Natanz nuclear facility and sabotaged their nuclear installations. Although no one has claimed responsibility for Stuxnet, it is acknowledged to be a jointly built American-Israeli cyber weapon.

'Regin' Telecom Hack (2010–2013)

It is suspected that the English Government Communications Headquarters (GCHQ) directed a cyber-attack using 'Regin' malware when targeting the



headquarters of Belgacom, Belgium's dominant telecoms provider. The company plays a crucial role in Europe and has partnerships with hundreds of telecommunications companies around the world.

Geographical distribution of 'Regin' Telecom Hack

The UK'S goal was supposedly to deeply infiltrate the Belgacom network to access communications of important customers such as NATO, the European Parliament and the European Council, as well as from clients of hundreds of international telecoms providers. The British agency has never confirmed or denied its involvement.

'Wiper' (2012)

How can a security company study malware that systemically wipes hard drives clean, leaving no trace of its own code? The global 'Wiper' hack perplexed security firms when it crippled networks in multiple countries. The malware algorithm destroyed hundreds of gigabytes of hard-drive data at a time, causing the machines to crash. It most notably hit computers in the Iranian Oil Ministry and the National Iranian Oil Company at a time of growing pressure on Iran's nuclear developments. Ukraine was the hardest hit country; the malware targeted its power companies, airports, banks, state-run television stations, postal facilities and large industrial manufacturers. Wiper shares characteristics with Stuxnet, which is why it is suspected to have been set in motion by Israel and the U.S.

Denial-of-service attacks on banks (2011-2012)

Attackers hit one American bank after the next. The perpetrators hijacked "clouds" of thousands of networked computer servers to perform DDoS, or denial of service attacks, that prevented customers from accessing online banking. The sophistication of the hack convinced Western nations that it was the work of Iran in retaliation for UN economic sanctions and the Stuxnet attacks. Carl Herberger, vice president of a security firm said that "there have never been this many financial institutions under this much duress." The attackers threatened that "from now on, none of the U.S. banks will be safe." Although Izz ad-Din al-Qassam Cyber Fighters took responsibility, U.S. officials say the group is just covering for Teheran.

Edward Snowden Leaks (2013)

In 2013, Edward Snowden, a former Central Intelligence Agency employee, leaked classified documents from the National Security Agency (NSA) revealing the United States had been cyber attacking international networks. Snowden said the NSA had over 61,000 hacking operations across the globe. "We hack network backbones - like huge internet routers, basically -

that give us access to the communications of hundreds of thousands of computers without having to hack every single one," Edward Snowden said.

'WannaCry' ransomware landing page

GCHQ was also found monitoring up to 600 million communications every day.

Sony Pictures Attack (2014)

In 2014, a hacker group named “Guardians of Peace” (GOP) hacked the film studio Sony Pictures and released confidential data, including personal information about employees and their families, unreleased footages, and much more sensitive information. They then used malware to erase Sony’s computer infrastructure, completely paralysing the Japanese company. The group demanded for Sonny to cancel the release of its film The Interview, a comedy on the North Korean leader Kim Jong-Un, threatening terrorist attacks at screenings. Sony capitulated, setting a dangerous precedent that victims can give in to cyber terrorist demands. U.S. officials, after careful evaluation of software used in the attack, alleged it was sponsored by North Korea. The country, however, has denied all responsibility.

‘DuQu’ and Iranian Nuclear Talks (2014)

The malicious ‘DuQu worm', linked to Israel and the U.S., struck at three European hotels where nations were congregating to discuss the details of the Iranian nuclear deal. Diplomats from the U.K, the U.S, China, France, Germany, and Russia, were present for the negotiations, though Israel from afar loudly opposed the plan to ease the restrictions on Tehran’s nuclear program. Israel was accused of spying on international negotiations on the Iran deal and using the intelligence gathered to persuade Congress to undermine the talks. Israel has denied being behind the attacks.

‘WannaCry’ Worm (2017)

200,000 victims and more than 300,000 computers were hacked in May 2017 by WannaCry’s ransomware worm. The virus, released by a group named Shadow Brokers, held computers hostage and demanded victims pay ransom to regain the files on their computers. All of the files on the person’s computer were encrypted and the only way to retrieve the information was to pay $300 in ‘WannaCry’ ransomware landing page bitcoins at the time of infection. If the user didn't pay within three days, the ransom doubled. After seven days, WannaCry deleted the encrypted files and all data was lost. Over 150 countries were affected. Parts of the United Kingdom's National Health Service (NHS) were striked at, causing them to only carry out emergency services during the attack. Spain’s Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries companies worldwide. The worm was linked the North Korean-affiliated hacking team Lazarus Group, who also allegedly orchestrated the Sony Attack in 2014. The

attack was destructive in nature and demonstrated North Korean intentions to inflict harm on Western systems. An American official said: ”The big lesson we learned from WannaCry, no matter who did it, is just how vulnerable, prone and exposed some of our critical pieces of infrastructure are.”

‘Shamoon' Virus (2017)

In 2012, computer virus Shamoon was launched against Saudi Arabian oil group Aramco’s computers, wiping data from 30,000 machines and destroying system files. It nearly obliterated its corporate IT infrastructure and brought the company close to collapse.

Shamoon re-emerged in January 2017. This time, it reportedly hit 15 government agencies and organizations. It stole over half a million confidential Foreign Ministry documents and even affected the Human Resources Development Fund’s computer systems. The United States accuse Iran for the hack but have never produced evidence.

American Presidential Elections (2017)

Russia is currently being accused of striking at the heart of American democracy: its 2016 elections. Many consider Putin tipped the election from Hillary Clinton to her opponent Donald Trump. The ODNI and the Department of Homeland Security (DHS) stated that Russian actors hacked the servers of the Democratic National Committee (DNC) and Clinton’s campaign chairman’s Google email account. Researchers claim the intrusions were masterminded by Russian teams named Fancy Bear, Cozy Bear, or the Dukes with an aim of discrediting the Democratic candidate. Russia, however, has repeatedly denied responsibility for any cyber attacks against America.

Major Countries and Organizations Involved

North Korea

Since the 1980’s, numerous resources have been poured into Bureau 121, North Korea’s central cyber warfare agency and one of today’s largest organizations. North Korea’s military primarily targets

South Korea, Japan, and the United States. Based in Pyongyang, it is estimated to have recruited nearly 6,000 full-time programmers. They have attacked South Korean banks, broadcasting companies, and nuclear reactor operators in 2013 and 2015. They are also thought to be behind the Sony Pictures and 'WannaCry' hack that spread to over 150 countries, putting thousands of lives in danger.

Kim Jong-Un is known for propelling North Korean cyber attack capacities

Iran

In the last seven years, three government funded computer viruses — Stuxnet, Flame, DuQu and Stuxnet — have stricken computers in Iran. As a result, the country has increased its force in the cyber warfare battle field. Over the past five years, funding for cyber security has been raised from $3.4 million to $19.8 million. In 2011, Iran allegedly masterminded denial of services attacks to disrupt oil companies in the Middle East as well as on the American finance industry. Amongst others, they also reportedly masterminded the 'Shamoon' virus that attacked Saudi Arabian oil groups in 2012 and 15 government agencies in 2017.

China

China is also a prominent cyber power. It is suggested that they directly employ 30,000 cyber pies and 150,000 private sector computer experts to strengthen their abilities. China's cyber warriors have launched numerous attacks; they hacked various Silicon Valley companies such as Google to exfiltrate key information. They also breached the US Office of Personnel Management in 2014 and are suspected to be partnering in North Korean cyber operations.

Russia

Russia's intelligence services decided years ago to make cyber warfare a national defense priority; it has therefore become a new sector in the Russian military strategy. Elite teams of computer hackers have been recruited to expand the Kremlin's interests through their highly advanced program. The country is strongly believed to have deployed cyber weapons to destabilize Georgia prior to their military confrontation in 2008. Russia is also accused of having organized the Yahoo breach in which 1 billion users had their account information stolen. The most current assertion is that Putin sponsored Russian hackers to steal data from the Democratic National Committee to ensure President Donald Trump's election to office.

Israel

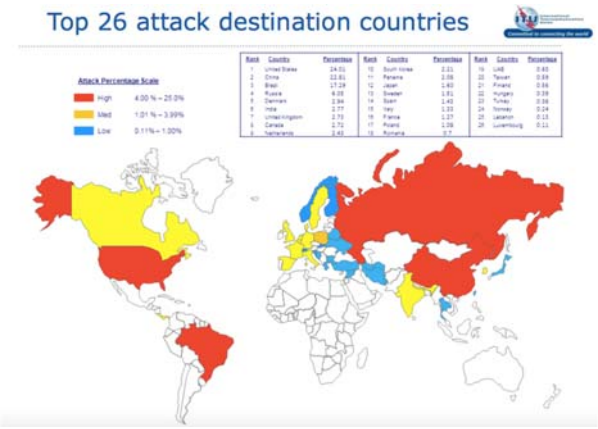
Israel has invested considerable resources to promote cyber security research. The Israel Defense Forces (IDF) aspire to base their power on advanced and technological solutions. In fact, the country has an estimated 10% of global sales of computer and network security technology. Check Point Software Technologies is a world leading Israeli multinational provider of data and network security software. A report that examined their cyber preparedness out of 23 countries awarded Israel the highest score (4.5 out of 5). Israel has been linked to the Stuxnet, Flame, Wiper, and DuQu attacks.

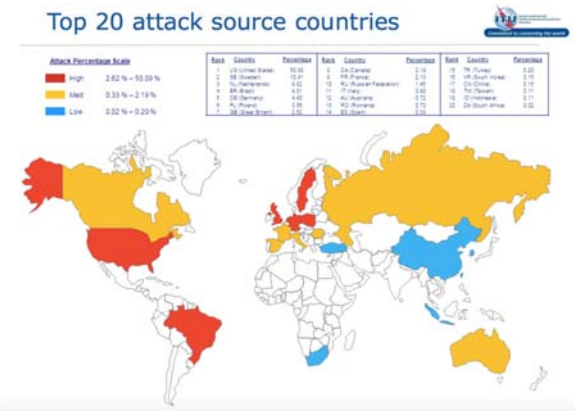
United States

Cyber terrorism is known as the “achilleas heel” of the United States. When U.S. director of National Intelligence, James Clapper, was asked about the threats faced by the United States, he placed cyber at the top. National Security Advisor, Condoleezza Rice explained the relationship between information technology security and U.S. infrastructure when she said: “Virtually every vital service — water supply, transportation, energy, banking and finance, tele-communications, public health — all these rely upon computers and fiber optic lines, switches and the routers that connect them. Corrupt those networks and you disrupt this nation.” In 2016, the U.S. initiated a Cyber National Mission Force with about 6,000 military personnel and 133 teams working to protect the nation’s critical infrastructure and key resources. The Department of Homeland Security (DHS) also plays a key role in strengthening American cyber defense capabilities. While it is protecting its own country, it has also been accused of attacking others. The Edward Snowden 2013 leaks revealed the NSA had been conducting hundreds of cyber operations. For instance, it has been held liable for the Stuxnet, Flame, Wiper and DuQu hacks alongside Israel.

United Kingdom

The United Kingdom is seen as the centre of cyber specialism in Europe with the launch of its new £1.9 billion national security strategy. Philip Hammond, Chancellor of the Exchequer said: “If we do not have the ability to respond in cyberspace to an attack that takes down our power networks, leaving us in darkness, or hits our air traffic control system, grounding our planes, we would be left with the impossible choice of turning the other cheek and ignoring the devastating consequences or resorting to a military response.” The U.K. has also performed offence operations. It was held responsible for the ‘Regin’ malware hack on telecom companies and for working with the NSA in its cyber operations.





Attack destination and source countries; red being the highest and blue the lowest

Timeline of Events

Date	Description of event
1965	Gordon Moore proclaimed “Moore’s Law” stating that computing power would increase exponentially. This foreshadowed its influence and its capabilities to cause international disruption.
August 6th, 1991	The Internet first became publicly available.
August 2008	Cyberattacks on the Georgian government, business websites, and network infrastructure disabled web-based communication. Shortly after, Russian forces invaded Georgia.
2010	‘Stuxnet’, the first cyber-attack that allowed hackers to yield real-world consequences, targeted Iran’s nuclear uranium enrichment facilities and hindered their progress.
November 2010	Britain announced it would dedicate $1 billion to build and bolster cyber defense.
2010-2013	Belgacom, a leading Belgian telecom company was hacked by ‘Regin’ malware. This enabled the attacker - presumably the British GCHQ - to acquire information on Belgacom customers which include NATO, the European Parliament and the European Council.
2011	China reportedly hacked Google, RSA Security, and other technology companies to obtain sensitive data.
2011-2012	Iranian hackers allegedly directed DDoS attacks against AT&T servers to disrupt oil companies in the Middle East.
2011-2012	A series of denial-of-service attacks on American banks devastated the finance industry. Clients could no longer connect to online banks, creating havoc.
2012	Shamoon malware — believed to be created by Iran — attacked the Saudi Arabian oil group Aramco’s computers.
2012	The ‘Wiper’ worm brought networks in multiple countries to a standstill when the algorithm encrypted computer data.

2012	The ‘Flame’ attack mainly affected Iran, Israel, the Palestinian Territories, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt. It infected systems to gain control of administrative accounts and government exclusive information.
2013-2015	North Korea was reported to have conducted cyber terrorism against South Korea. In the year 2013, North Korea reportedly attacked three South Korean broadcasters and a major bank. The cyber-attack froze thousands of computers and ATM’s around the country. Next, in 2015, North Korea was blamed for a data breach on Korea Hydro and Nuclear Power - the company that operates South Korea’s 23 nuclear reactors.
2013	Edward Snowden first exposed NSA cyberterrorist operations. Some of his leaks included the disclosure that the United States carried out 231 offensive cyberattacks in 2011.
2013	It was disclosed that the Iranian government attacked against 50 targets in 16 different countries.
2014	Russian hackers were accused of having organized a cyber-intrusion of the US State Department.
2014	The US Office of Personnel Management was allegedly hacked by the Chinese. This attack led to a massive loss of personal data, including 21.5 million details of U.S. Citizens.
2014	The Sony Pictures company was hijacked.
2014	‘DuQu’ malware made its way to European hotels in which diplomats were engaging in talks on reducing restrictions of Iran’s nuclear program.
2014	Yahoo was troubled with one of the most powerful cyber terrorist attacks of all time when hackers stole data from more than one billion customer accounts.
2015	American President Barack Obama and Chinese President Xi Jing Ping reached a cyber-security agreement.

2016	The FBI held North Korea accountable for pirating $81 million from the Bangladesh central bank's account. The incident showcased just how open to attack the online finance world is.
2016	The United States announced it would use its cyber capabilities against the Islamic State (ISIS) as the terrorist organization heavily relies on the information age to carry out their ambitions. The U.S. aims to prevent ISIS from communicating with one another, attracting new fighters, and are also trying to disrupt their ability to circulate orders and conduct operations with their highly sophisticated hacking. Potential recruits may also be deterred if they come to worry about the security of their correspondence with the militant group.
May 12th, 2017	Over 150 countries and 300,000 computers were hacked by 'WannaCry' ransomware.
2017	Shamoon' hit 15 government agencies and organizations, including major oil companies.
2017	Charges against Russia proclaim they took part in cyber terrorism by interfering with the 2016 American Presidential Elections. Hackers presumably discredited Hillary Clinton to sway voters towards Donald Trump. Russia, however, has denied all accusations.

Relevant UN Treaties and Events

- Developments in the field of information and telecommunications in the context of international security, 4 January 1999 (A/RES/53/70)
- Combating the criminal misuse of information technologies, 22 January 2001 (A/RES/55/63)
- Creation of a global culture of cybersecurity, 31 January 2003 (A/RES/57/239)
- Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 30 January 2004 (A/RES/58/199)
- Aviation Security, 22 September 2016 (S/RES/2309)

Main Issues

Unpreparedness leading to national paralysis

Cyber defense systems are currently outdated and decentralized; most governments and companies do not have strong preventative or response plans. Virtual attacks can have physical consequences in a matter of seconds, leading to complete standstills in key sectors. Cyber terrorists have the power to dismantle a public utility or power plant that provides crucial water or electricity. They could therefore prospectively cut those indispensable resources in a country or area. Moreover, telecommunication systems are a target they could exploit to disable the transmission of information. One could only imagine the consequences of compromised institutions that run our countries like infrastructure, our economies, our security systems, and so on. The power for disruption is unimaginable; strategizing the strengthening of our vulnerable fronts is of utmost importance.

Cyber arms race

Just like nuclear weapon proliferation has increased over the decades, countries will also spike their cyber capabilities. All players want to be ready and equipped if needed. The nuclear arms race lasted for most of the twentieth century. However, Mikko Hypponen, F-Secure's Chief Research Officer believes we are "at the beginning of the next arms race. This time it's going to be a cyber-arms race." Whether having cyber capacities is a deterrent or not, it is clear that the more sophisticated the technology gets, the more destructive it can become.

Previous Attempts to solve the Issue

National attempts

In March 2003, the Department of Homeland Security initiated Liberty Shield, a national plan designed to increase protection for America's infrastructure. Its technology aggressively monitors the internet for signs of potential cyber terrorist attacks and information breaches. The UK has also published its "Nations Cyber Security 2016-2021 Strategy" in which it will invest £1.9 billion in defending systems and infrastructure to deter adversaries. Among others, the EU has also taken great strides. Since the adoption of the EU Cybersecurity Strategy in 2013, fighting cybercrime is one of three priorities under the new European Security Agenda. Russia has also elevated their protection by using a closed government network called RSNet. Every employee has their own secure work account that can only be accessed from a special IP address using a designated computer. They have also recently designed a "crypto phone" which allows users to use encrypted phone services.

United Nations Resolutions

Several resolutions regarding security in our information technology have been discussed at the United Nations. These include A/RES/55/63, A/RES/57/239, and A/RES/58/199. The resolutions urge all nations to take part in international cooperation and communication with one another to achieve cybersecurity and the protection of critical information infrastructures. They specify spreading awareness of the dangers

cyber terrorists pose and encourage States to share their strategies and best practices to facilitate the defense process for other nations. Moreover, they outline preventative procedures and the installment of emergency warning networks regarding cyber-vulnerabilities. Finally, they state that all stakeholders should conduct risk assessments of essential sectors subject for re-evaluation following a 1 to 2 year period.

US-China Cyber Agreement

In 2015, Chinese President Xi Jing Ping was hosted by Barack Obama at the White House. After years of Chinese cyber-attacks plaguing the United States and the Snowden leaks exposing that the U.S. had been conducting cyber operations in China, the two leaders finally came to a consensus. They agreed to never cyber-attack one another and concluded they would engage in dialogue on fighting cybercrime and notifying the international community when it arises. Cybersecurity experts at the Council on Foreign Relations, however, said that building on the agreement would not be easy as trust is rare, especially in cyber space. Indeed, it remains unclear whether China or the U.S. have reduced intrusions in each other's systems since then.

International Telecommunications Union (ITU) Efforts

The ITU, a United Nations agency specialized in communications and technologies, has worked alongside nations and the private sector to help further cyber security preparedness. One of their great achievements was initiating The Global Cybersecurity Agenda (GCA), which was launched in 2007 by their Secretary General. It remains a unique framework that encourages nations to build on and improve existing cyber intrusion combat efforts through personnel training and the development of common strategies. The ITU also helped orchestrate the the International Multilateral Partnership against Cyber Threats (IMPACT), the first public-private partnership against cyber threats. It serves as a politically neutral global platform that brings together leaders of governments, industries, and international organizations to pool efforts towards cyber security response. They anticipate emerging and future challenges with shrewd plans of action.

Possible Solutions

Cooperation

Joint action is also necessary - between nations and amongst the public and private sectors. Many oil companies, electricity companies, communication companies, financial institutions, or technology firms are not controlled by the government — yet attacks against them can prove far more dangerous. Since private holdings manage dozens of national critical infrastructures, efforts will require trusted partnerships

between the government and private sector. They will need to combine resources to reinforce cyber infrastructure, train personnel in analytics, and outline procedures enabling the rapid prevention, detection, and response to security incidents. International partnerships must also take shape. Allies should share information about each other's vulnerabilities and conduct research; only in this way will security technologies exponentially increase in power and effectiveness.

Cyber disarmament

It has been said that the new arms race will consist of building up on destructive cyber technology. If this is the case, some believe shutting down all offensive cyber development is the only way to prevent chaos. Others claim that having nationwide cyber capabilities serves as a deterrent - just like nuclear proliferation deters nations from attacking each other due to fear of retaliation. Moreover, it is argued that even if nations "disarmed" online, North Korea, China, and Russia never would, leaving all others vulnerable to their hostilities. Although complex and subject to debate, cyber disarmament is a matter that is being discussed and must be noted. Cyber terrorist attack's imminent dangers are an integral part of the 21st century. How will our nations approach this new frontier?

Bibliography

"Belgian Press Reveals British Hacking of Belgacom." *EURACTIV*. EURACTIV Network, 15 Oct. 2015. Web, https://www.euractiv.com/section/digital/news/belgian-press-reveals-british-hacking-of-belgacom/

Breene, Keith. "Who Are the Cyberwar Superpowers?" *World Economic Forum*. WEF, 4 May 2016. Web, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Gibbs, Samuel. "Duqu 2.0: Computer Virus 'linked to Israel' Found at Iran Nuclear Talks Venue." *The Guardian*. Guardian News and Media, 11 June 2015. Web, https://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks

Hardy, Nicole Perlroth and Quentin. "Online Banking Attacks Were Work of Iran, U.S. Officials Say." *The New York Times*. The New York Times, 08 Jan. 2013. Web, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html

Hern, Alex, and Ewen MacAskill. "WannaCry Ransomware Attack 'linked to North Korea'." *The Guardian*. Guardian News and Media, 16 June 2017. Web, https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group

Kramer, Andrew E. "How Russia Recruited Elite Hackers for Its Cyberwar." *The New York Times*. The New York Times, 29 Dec. 2016. Web, https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html

Lee, Dave. "Flame: Massive Cyber-attack Discovered, Researchers Say." *BBC News*. BBC, 28 May 2012. Web, http://www.bbc.com/news/technology-18238326

Lever, Rob. "US Charges Two Russian Spies in Massive Yahoo Cyberattack." *Yahoo! Tech*. Yahoo!, 15 Mar. 2017. Web, https://www.yahoo.com/tech/us-charges-two-russian-spies-criminal-hackers-yahoo-164205521.html

Levine, Mike, and Emily Shapiro. "How Russian Agents Allegedly Directed Massive Yahoo Cyberattack." *ABC News*. ABC News Network, 15 Mar. 2017. Web, http://abcnews.go.com/US/russian-agents-facing-charges-yahoo-hacking-attacks/story?id=46142396

Matharu, Aleesha. "Cyber War: A Guide to State-sponsored Digital Assaults." *CatchNews.com*. N.p., 8 Sept. 2015. Web, http://www.catchnews.com/international-news/cyber-war-a-guide-to-state-sponsored-digital-assaults-1441638811.html

Park, Madison, and Dana Ford. "North Korea Denies Being behind Sony Hack." *CNN*. Cable News Network, 14 Jan. 2015. Web, http://edition.cnn.com/2015/01/13/asia/north-korea-sony-hack/

Riley, Charles, and Samuel Burke. "WannaCry Cyberattack Linked to North Korea." *CNNMoney*. Cable News Network, 16 June 2017. Web, http://money.cnn.com/2017/06/16/technology/wannacry-north-korea-intelligence-link/index.html

Sanger, David E., and Nicole Perlroth. "Iranian Hackers Attack State Dept. via Social Media Accounts." *The New York Times*. The New York Times, 24 Nov. 2015. Web, https://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html

Sanger, David E. "U.S. Cyberattacks Target ISIS in a New Line of Combat." *The New York Times*. The New York Times, 24 Apr. 2016. Web, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

Smith, Ms. "Saudi Arabia Again Hit with Disk-wiping Malware Shamoon 2." *CSO Online*. CSO, 24 Jan. 2017. Web, http://www.csoonline.com/article/3161146/security/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html

Szoldra, Paul. "Everything Edward Snowden Revealed in One Year of Unprecedented Top-secret Leaks." *Business Insider France*. Business Insider, 16 Sept. 2016. Web, http://www.businessinsider.fr/us/snowden-leaks-timeline-2016-9/

US & Canada. "Edward Snowden: Leaks That Exposed US Spy Programme." *BBC News*. BBC, 17 Jan. 2014. Web, http://www.bbc.com/news/world-us-canada-23123964

Volz, Dustin, and Julia Edwards Ainsley. "Russians Targeted 21 Election Systems, U.S. Official Says." *Reuters*. Thomson Reuters, 21 June 2017. Web, http://www.reuters.com/article/us-usa-cyber-congress-idUSKBN19C1Y3

Wagenseil, Paul. "Israel, NSA May Have Hacked Antivirus Firm Kaspersky Lab." *Tom's Guide*. Tom's Guide, 10 June 2015. Web, https://www.tomsguide.com/us/kaspersky-hack-israel-nsa,news-21084.html

Appendices

Beaver, Michael. "The United Nations and Cyberwarfare." *Global Risk Advisors*. Global Risk Advisors, 10 Apr. 2017. Web, https://globalriskadvisors.com/blog/united-nations-cyber-warfare/

Frost, David. "Espionage Expert Offers Five Viewpoints on State-sponsored Hacking." *The Resource for Data Security Executives*. N.p., 4 Apr. 2017. Web, https://www.cso.com.au/article/617077/espionage-expert-offers-five-viewpoints-state-sponsored-hacking/

Dunn, John E. "The World's 10 Most Dangerous Cyberwarfare Attacks." *Techworld*. N.p., 14 Mar. 2015. Web, http://www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660/

OWL Cybersecurity. "A Survey of Nation State Sponsored Hackers." *OWL Cybersecurity*. N.p., 30 Apr. 2017. Web, https://www.owlcyber.com/blog/2017/2/23/nation-state-sponsored-hackers

Sanger, David E. "In Cyberspace, New Cold War." *The New York Times*. The New York Times, 24 Feb. 2013. Web, http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html