**Human Rights, Digital Rights, and Security: Public Policy for the 21st Century Cyberspace**

Throughout history, humanity has relied on technology to survive. From bronze and steel to paper and steam machines, empires have risen and fallen with their creations, leaving them to be implemented by others in history. This century, the biggest technological advancements are the intangible digital media created through computers and innovations pertaining computers themselves, such as the smartphone - essentially a pocket computer with cellular capacities - and wearable technology. Dependence on technology for survival has always been a thing: it is no coincidence that times of war and conflict are hotspots for development. These advancements have always been for a better quality of life by alleviating and solving problems, or giving alternative ways to achieve something, but have mostly pertained themselves with factors external to humans. Social media and the internet changed that: technology is now supplying essential human needs - such as social interaction - and rapidly changing how we engage with the world around us. In theory, that may sound like a good thing; in practice, these practices are ripe for abuse.

The first computers were built in the UK and the US, and their developments have stayed there for the most part. With the creation of the microprocessor, computing took a large step forward in the 70s by making personal computers commercially available, and so a large part of the business environment; up until that point, computers were large, bulky things with very specific scientific or technical applications, and not suited for the general public. In the last 50 years, personal computers and their integration into daily life have grown dramatically, going from business applications and education to entertainment and socialization, with the internet facilitating communication and information sharing. Mobile computing made it triple fold, as these devices are built specifically for on-the-go use (and so are always on/always connected), with have specific sensors and tools to permit this. For users, this 24/7 availability permits on-demand content. For malicious parties, this provides a bounty of information to intercept, steal and misuse.

Cybersecurity - the impenetrability of a service or program - is a relatively new field. Surging in the 90s with telephreakers (people who intercepted phone calls and telecommunications systems) and hackers (people who changed programs without the user knowing to intercept information), it started with some parties’ curiosity over the internal working of a system but quickly developed into much more: normal and inoffensive questions such as ‘What type of protocol does this use?’ and ‘What frequency does this sound work on?’ became ‘Can I trick the system to get access into this secure platform?’ and ‘How much can I damage a computer and/or information with this program?’, and engaged in illegal - or at the very least, legally grey - activities. Companies started to pay attention to how secure their systems were only when they started to be exploited and demanded action from the law to account for the damages they had received. Laws pertaining information access and computers, such as the Uniform Computer Information Transactions Act, stopped most malicious actors from going after companies, but it had the unintended consequence of them changing their targets instead of stopping their activities. Because companies are under no requirements, legal or otherwise, of making their platforms secure, most of the products they deliver come with a plethora of vulnerabilities that people can exploit to get information with unauthorized access, without the product or user knowing about it. As such, if a malicious actor attacks the company that made the product, he’d be in trouble, but if he attacks a user that has this product, there is no harm done to the company and so there’s not much to do. While this is concerning by itself, the real harm comes when we consider that anyone with sufficient knowledge could do this, without wanting to steal credit cards or perform identity theft.

States have an interesting relationship with the law, in that they are both blessed and cursed by it. Throughout history, the reality of states not representing their citizens’ will or needs has been more common than expected, with dubious politicians changing the law to allow their schemes to take fruit or give leeway to other interested parties. They can pass or change laws that suit their needs. But there are also other parties that can pass or change laws, that can advocate for citizens, and will limit the state’s reach if it were to have ill intentions. States often go up against the thin line of what is legally admissible to get away with what they want to do, often in the name of national security. The examples are many and mostly controversial, as they usually result in human rights violations: take, for example, the CIA’s Enhanced Interrogation Techniques acquired after 9/11 with the War on Terror as a motive. This state sponsored torture program has been widely criticized and condemned, but has not resulted in any repercussion, legal or otherwise. In information security and computing, there are little laws to protect citizens. What laws exists are there for corporate interest or protection of essential services and infrastructures. Users have nowhere to go for protection and must blindly trust their products’ manufacturers to properly secure their information, or be savvy and knowledgeable on the subject enough to properly protect themselves.

Knowing that there’s nothing stopping or limiting them, several states have actively participated in a widespread information interception of their citizens, other states, and other states’ citizens, with goals such as national security, warfare, destabilization, economic interests and political campaigns. Because computers and the internet are inherently anonymous, it is difficult (although not impossible) to pursue and prove that attacks have come from one or other state, but even if they do, there is next to no protocol on how to handle these situations. Where the destruction of physical resources is a clear act of war, the interception and compromise of information sources that do not hold physical value and/or are not owned by the state has not been seen before and international law, treaties and protocols have not yet completely understood the implications and realities of these actions. Like the gold rush in the United States and the concept of the ‘Wild West’, actions performed through the digital space are first-come-first-serve, and there is no medium or platform for accountability. Cyberattacks are not correctly address as physical attacks are, human rights violations through surveillance are allowed and facilitated by law, misinformation campaigns and psychological warfare are not taken seriously. The risks of human rights violation come not only from the controversial mass surveillance programs, but also from state conflicts and new warfare mechanisms that can threaten the way civilians lead their lives.

**COUNTRY/REGION BACKGROUND**

US

In 2013, Edward Snowden uncovered the mass surveillance programs the NSA (National Security Agency) was engaging in. With the motivation of national security, the NSA enlisted several top tech companies (Google, Apple, Microsoft, among others) to provide information about their users and customers when needed, gaining access to email, video and voice chat, videos, photos, voice-over-IP chats (like Skype), file transfers, and social networking details. This program, known as PRISM, targeted US citizens and foreigners alike and collected massive amounts of information both in content and technical details, such as what devices were used, where they connected, what accounts were active, etc. Having originated there, most of the internet’s traffic goes through the US, which facilitates worldwide data collection.

PRISM wasn’t the NSA’s only surveillance program, although it was one of the few to be declared unconstitutional, with several lawsuits against the NSA, President Barack Obama, and the United States. The US has history of state sponsored surveillance and spying programs, such as the Black Chamber/Cipher Bureau created during WWI; the NSA’s behavior is not new nor unexpected. What is alarming, however, is the extent the organization will use and exert its influence as a state organization to both carry out data gathering with an unprecedented reach and to infiltrate and intercept private owned media that facilitates communication and daily life, with and without the owners knowing about it. One of the most successful initiatives was, for example, to intercept digital infrastructure (switches, firewalls, routers, laptops, computers, etc.) mail packages and implant them with devices that allowed for remote connection and unlimited access to any and everything that would pass through said device. This might or might not have been done with the vendors’ or mailing companies’ knowledge, but other examples prove that even if they would have known, there would not have been much of a choice for them: a great part of the success of the PRISM program was its data sources, which were predominantly coming from high ranking and widely relied upon tech companies, such as Microsoft, Google, Apple and Yahoo. These companies were forced to give data access to the NSA upon request and were forbidden to disclose or share any information about it.

The revelation of these surveillance programs gave way to a global debate around government control and accountability, as well as the analysis on how human rights can be and are violated with digital media. Tension between the US and several other countries grew as information was disclosed on which countries, dignitaries and leaders were spied; in the 5 years passed, the notion of being surveilled right now is not as alien as it was before the NSA leaks. There is a growing distrust in state agencies and the government, as citizens realize that those tasked with protecting them are the ones harming them.

UK

The GCHQ (Global Communications Headquarters) is the UK’s equivalent of the US’ NSA, and both work closely to share resources and information. With the disclosure of the NSA documents, information on other countries’ own programs was also revealed: in the UK’s case, this is Tempora. While the NSA is mostly concerned on metadata to create a traceable digital fingerprint - an online presence that can be identified belonging to a single source, no matter where it arises - of specific citizens and foreigners, GCHQ is interested on both metadata and data without discriminating between citizens, foreigners, and potentially malicious actors against the state. The UK government uses listening posts, probes, and arrangements with private companies - both by state orders and economic arrangements - to collect information on anyone and is thought to have a much larger database than the NSA, despite the latter having a larger reach both in geographic areas and infrastructure access. It is estimated that the amount of data collected by each probe (47 in total across the country) is of 10 Gigabits per second.

While the NSA relied on spying and interception techniques on private companies, GCHQ had access to the core infrastructure of the UK’s internet services, such as the fiber optic cables used by ISPs (Internet Service Providers), which allows them for much broader and deeper monitoring. Even if condemned and criticized, after several lawsuits the NSA shares information on the type of information it collects, how it collects it, and if it ever uses it, it will mention the source. With GCHQ, there is a notorious silence on how and what is done, and has led to at least one diplomatic incident. A coalition of 14 human rights groups and privacy organizations, including Amnesty International, Liberty, Privacy International and Big Brother Watch, took the UK to court through the ECHR (European Court of Human Rights) in October 2018. The ruling dictated that GCHQ was in violation of human rights, specifically, article 8:

*“By a majority of five to two votes, the Strasbourg judges found that GCHQ’s bulk interception regime violated article 8 of the European convention on human rights, which guarantees privacy, because there were said to be insufficient safeguards, and rules governing the selection of “related communications data” were deemed to be inadequate.”* (The Guardian, 2018)

In an interesting but perturbing note, the same court ruled that the sharing of this information between states is not in violation of human rights:

*“The regime used by the UK government for sharing intelligence with foreign governments did not violate either article 8 or article 10, which guarantees freedom of speech. Not was there any evidence, the judges said, to suggest that the intelligence services were abusing their powers.”* (The Guardian, 2018)

Five Eyes Intelligence Alliance

Created in the Cold War, the growing landscape and reach of digital technology provided enough reasons for the program to remain active well beyond its original intentions of unity against the USSR. The Five Eyes Intelligence Alliance is formed by the UK, US, Canada, New Zealand and Australia, with the purpose of sharing resources for intelligence and information gathering. A particular usage of this alliance is the circumvention of local laws: states allow other members in the program to spy on their citizens, and as external agents, they will be held accountable to local law as much as the state wishes it. If the state is condoning it, there is no way for citizens to know about it and will in fact protect the external state and will not hold it accountable as it benefits them. The main initiative for surveillance is called ECHELON, created to monitor and intercept private and public communication channels, including satellite interception.

Knowing that this program exists, and that this is how it operates, it is highly concerning that the ECHR did not consider these practices in relation to the GCHQ’s surveillance a violation of human rights, and is even contradictory: following the same ruling and the operation techniques of the program, the implication is made that it is inadequate for states’ to spy on their own citizens, but it is acceptable if they spy on other countries’ citizens. It may be the case that it was not considered a violation because it is a cooperation program that relies mostly on each country’s sovereignty and the way they chose to interpret other countries’ actions against them, but the fact that this is exploited to circumvent local law that is not applicable to the foreign country in favor of the local country is extremely concerning.

China

China’s economic rise was a surprise to the western world, who thought that it would eventually crumble under its own weight in the same way that past authoritarian/communist states have. Due to differences in production cost, most of the western tech companies outsource their manufacturing procedures to cheaper countries such as Vietnam, India and China, the latter being the biggest client. With decades of training by working in these factories, Chinese tech companies arose quickly and prominently with a strong presence in the area, and by law, they are required to meet quotas for the government’s usage. Almost all the physical technology created in the west is available to China, not by buying but rather by copying and customizing for their own needs. Where in democratic countries the state is held accountable (or, at least it is in theory) by their citizens and with the division of power, China’s authoritarian government can effectively do as it pleases.

Internet access in China is severely restricted. Specific websites - such as Facebook and Google - are blocked state-wide, and only government sponsored platforms are allowed in their place. Content curation is widespread and rampant with state actors deleting any and all information criticizing or putting the government in a bad light, harassing the creators of said information and depriving them of internet access as a punishment. Certain technologies that would allow for circumvention of these limits are also forbidden, such as VPNs (Virtual Private Network) or TOR (The Onion Router) connections, which allow for connections to originate from elsewhere to avoid the content limitation. China has also made it clear to external tech companies that if they want to do business with the state, they will do it China’s way, or they will not do it at all. Google pulled out of China about 5 years ago due to the concern of human right’s violation, but what was seen as a good move from the tech giant turned out to be a secret project called Dragonfly, there Google created a custom version of its search engine tailored to the Chinese state’s limitations. The program was eventually cancelled out of the widespread and internal criticism.

Beyond the limit of information access, perhaps the biggest concern of China’s use of technology is the real-world panopticon it was created in Beijing. With the use of artificial intelligence, machine learning, facial recognition, cameras in public (and private) spaces and identity tracking, the state can pinpoint a person’s location and activities at any moment. This, mixed with their large body of police and military personnel in public spaces, allows for an almost immediate response to any state order, such as detaining a journalist or locating a dissident. Given the country’s not-so-friendly history to criticism and their current practices, the panorama for free speech and privacy is bleak and could get worse if China’s influences continue to grow and affect other countries and big companies.

Russia/Ukraine Conflict

In what is recognized as the worst cyberattack in history, Russia has engaged with Ukraine in multiple conflicts that have escalated to the latter’s allies. What started as an armed conflict with the annexation of Crimea in 2014, Russia has since harassed Ukraine in different ways by affecting their infrastructure and economy with different types of attack. The malware NotPetya was created by Russian hackers to target as many Ukraine computers and systems as possible by targeting Ukraine’s IRS tax program and exploiting a vulnerability that allowed them remote access and code executing. The malware was highly destructive by encrypting all information in computers in a one-way function that does not allow for decryption, basically destroying the information that is stored in the computer. The impact was enormous: while the infection vector was the IRS program, the malware propagated through networks, reaching systems that might not have had the program installed. Given that some networks go beyond national borders, this also impacted neighboring countries and companies that operated in Ukraine with offices elsewhere.

Traditionally, the destruction of physical resources has been considered an act of war, but the destruction of core infrastructure essential for digital operations is not physical and so not held to the same standards. Even with great economic loss (it is estimated the total cost of the NotPetya attack was around 10 billion dollars) and the active endangerment of civilian lives (banking systems were completely offline and supply lines were cut off, among other issues), the world and law do not respond to cyberattacks with the same stance it regards traditional attacks. This puts civilians at risk and makes them defenseless in times of warfare: where traditionally an army will defend the country in times of war, very few countries have tech teams dedicated to cyberdefense.

**CURRENT HUMAN RIGHTS CHALLENGES OR ABUSES**

Attacks to civilian resources

A clear example of how much can civilians be impacted by cyberwarfare is the NotPetya case, where systems were paralyzed and people were left without access to core resources by limiting their access to money, which in turn limited their access to food, water, electricity and essentially anything they might have to pay for to access. A more terrifying implication, however, is the possibility of targeting specific resources, such as hospitals and nuclear plants, to create widespread damage. Where traditionally an attack would happen with bombs and missiles and are easily traceable by intercepting plane communications and/or looking at the remains and technology used, cyberattacks are inherently anonymous and much harder to trace. If a state decides to target healthcare systems, which are notorious for their lack of security and outdated components, there is virtually nothing stopping the resulting life loss out of mixed records, incorrect dosages and/or medicines, and procedure changes that could easily occur with simple attacks. The damage would be irreversible for the human lives involved, would jeopardize the lives of other people that could at any moment depend on these systems, and would require a lot of effort to clean up, as dealing with sensitive information such as health records is very delicate. Similarly, if a state decides to infiltrate a nuclear plant and mess around with its industrial control systems, a nuclear reactor meltdown would not be too outlandish to happen, and the resulting radioactive fallout would have disastrous consequences on human lives, flora, fauna, and quality of life. This particular example could have happened when the US hacked Iran’s nuclear programs, with the difference that the motive behind the attack was not to cause damage to the lives of people and places (as could happen in an actual war) but rather to disable and destroy Iran’s nuclear capacity; as a result of the infiltration, around 35% of Iran’s nuclear resources were forcibly degraded beyond repair.

Destabilization of government structures

With the 2016 election meddling of Russia, the US government has been in a constant state of disarray and conflict. Civilian trust in state agencies is at a very low point, partisan conflicts are growing, and the administration’s movement towards deregularization is concerning. What is most interesting about the meddling is how Russia engaged in psychological warfare and misinformation campaigns to create conflict in the population and used cyberattacks in state agencies (such as the DNC) to further confuse people. It did not directly attack the state, but by disorienting people’s views and opinions and sowing distrust and discord it destabilized the country and left it in a vulnerable position.

Beyond the political motivations and realities that this campaign created, the misinformation campaigns had adverse effects on civilian’s habits, thoughts and opinions. One of the points of Russia’s misinformation campaign of decades in the making is the Anti Vaccine movement, where false information and claims on the risks of vaccines were shared to vulnerable communities, thus resulting in a great number of children not being vaccinated against previously eradicated diseases like the whooping cough. The number of people in the United States not vaccinated is now high enough that there is a very credible potential loss of herd immunity, where enough members of the population are immune to a disease that even if one gets sick, it will not be transmitted to enough individuals to be a disease vector. This can lead to a very dark reality; there is a reason that biological warfare is condemned, and yet this vulnerability of people is not considered biological warfare, even if in the long run it could have the same effects.

Censorship and repression

With China as the biggest offender, repression and censorship through digital channels are rampant. Persecution of journalists and political activists is very common, and repercussions towards speech towards the government is harshly and immediately punished. The lack of free speech and security are classic examples of human rights violations commonly associated with non-democratic governments, but the reach it has and the speed by which it is enforced is unprecedented and highly concerning. Where in the past dissidents had the real possibility of hiding, in the present there is nowhere to hide as everything is interconnected and has a 24/7 feed.

**IMPLICATIONS AND REALITIES**

Lack of definitions, language, accountability and repercussions for attacks

Perhaps the biggest challenge in cybersecurity and international relationship is the lack of protocols surrounding them. There is no clear definition on what exactly constitutes as a cyberattack, and attackers are not held accountable for their actions nor do they suffer any consequences. Economic sanctions are usually taken against a country when it engages in concerning behavior; perhaps the list should grow to include these types of attacks too.

While there are documents that include the implications and uses of cyberwarfare into their bodies, these are not legally binding or used worldwide. The Wassenaar Arrangement allows for the limitations of dual-use technologies - computers and telecommunication devices amongst them - by requiring countries to report how they use these items and how much of them to they have. It is a good start, but again, it is not a treaty and so not legally binding, and it is not widespread adopted, with several key players missing. Very few documents exist to account specifically for cybersecurity; while a call from the information security community for a ‘digital Genova convention’ has been around for more than a few years, lawmakers have yet to respond and account for the ever changing landscape of possibilities not contemplated with current law. Some have tried to include digital media in existing documents (like the Wassenaar Arrangement) or create coalitions to work on the problem together (like the UN’s Internet Governance Forum), but hard measures on the subject are yet to be taken.

Considering that the biggest players - US, Russia, and China - have decade long tensions between them, the chances of getting all of them to agree on the terms and protocols to limit cyberwarfare are slim. This was the same issue the United Nations faced when creating its Security Council, and it solved it by granting the powerful countries a veto to overturn decisions made by the majority. This is the biggest flaw in the UN system, and would make any digital security council equivalent almost completely ineffective if most of the concerns on cyberwarfare come from the countries that would hold the vetoes.

Technology is done with private sector, lack of regulations

Computer science, unlike other major fields, has only been around for the last century, with what we consider modern computers and the widespread use of the internet being around only for the last 50 years. Most of the technological developments surrounding computers and the internet have happened in the United States, country that is notorious for its protection of the economy, market and private sector. Other fields have regulations to protect consumers of the potential negligence of vendors and producers, such as agriculture, telecommunications and car manufacturing, but there is a notorious lack of accountability for tech companies’ shortcomings in serving their customers in the way they should. Data breaches are very common, which put millions of people at risk for other types of crimes against them by revealing sensitive information such as credit cards, addresses, social security number, bank accounts, and other types of information specific to the type of data breach; yet there is no repercussion against a company that had a poor enough security to allow for this. If an account is hijacked, hacked, deleted or something intercepted, very few companies have protocols or means to allow consumers to regain control of their media, and impersonated accounts can have disastrous consequences for people. In broad terms, a company’s accountability for security is as far as it costs it money; data breaches and hacks create bad reputation and can taint a company’s image and can make it lose customers.

Information security is seen as a cost with no economic value. If anything, it is an expense that has no monetary return and so there are few pushes towards making products or infrastructure secure. In last few years, companies have been scrambling to make up for years of gross mishandling of the security of their products after realizing how dangerous data breaches can be for their image and hacking campaigns can damage their infrastructure. But even with their movement to action, there is no standard to what is and is not secure enforced by the state, as there is for, say, food. Unless companies are held accountable from the start, the call for security can still go south quickly if it is seen as a calculated risk in terms of economic gain and loss, instead of a responsibility towards its users.

Almost no Redundancy

Most of the world’s digital media relies on the internet to operate, with the rise of ‘the cloud’, virtual machines, X as a service, and in general, outsourcing of technologic costs. Users, too, require internet for even the most basic of things, such as editing a document, playing a game or listening to music. Content is almost never stored locally and depends on the existing internet connection for functionality and access. But what if the internet were to disappear? While this scenario is a bit unlikely, the question still leaves a nightmare to envision, with most if not all services by both public and private organizations losing functionality with lack of connection.

Most technical fields recognize the importance of redundancy systems; the same approach should be taken in computer systems. Not all networks are the internet, and there are certain things that should be stored locally for protection. With NotPetya, the world got a taste of how the permanent and dependent connection of all computers can be very dangerous, and in fact the only defense mechanism most got towards the malware was to disconnect machines from the internet forcibly.

**PROPOSED POLICY RECOMMENDATIONS OR INTERVENTIONS**

The amount and type of actions to be taken to allow for the digital space to account for human rights is vast, but the most important and urgent ones have been discussed as scenarios in this paper.

State regulations should enforce - or at least encourage - security to be taken seriously, and state defense should account for the potential problems of the dependency on the private sector for their core infrastructure, as well as the potential spillover to trade partners in the event of a breach or attack, which in turn could create international incidents.

Specific tools whose only purpose is to damage, intercept, destroy or infiltrate a system with unauthorized access, should be considered weapons and their access should also be monitored. While some scenarios of this have been accounted for with the Wassenaar Arrangement, there is no regulation on who can access the technology and under what reason, nor is there any limit on who can create it. This question is very difficult to answer, as anyone with the sufficient knowledge and skill can build a program with enough destructive power to be considered a weapon. For instance, a popular tool to steal accounts and gain access called ‘mimikatz’, was created as a proof of concept by a civilian, with no ill intentions; but it was made widely available, for free, to anyone, and has been used and misused multiple times to hijack accounts. Should this be considered controversial, in the same way that 3d printed guns were a few years ago? Would individuals need a license to create and distribute these types of material, like a doctor or a lawyer need to practice their profession? There is no easy answer.

The adoption of international treaties for cybersecurity and cyberwarfare is paramount. The Wassenaar Arrangement update on dual-use technologies is one of the many changes that should be done to existing treaties, protocols, laws and conventions to account for the misuses of technology. Of particular mention, however, is a document called the Tallinn Manual, created in 2007 in Estonia by a group of cybersecurity experts after an incident in said country. This document explores how international law - particularly, the jus ad bellum and international humanitarian law - apply to cyber conflicts and cyberwarfare. This non-binding academic research shows the sort of things states need to account for and be responsible for, with the 2017 update (known as Tallinn 2.0) detailing the way other types of laws could fall into this spectrum, including elements such as law of state responsibility, the law of the sea, international telecommunications law, space law, diplomatic and consular law, and, with respect to individuals, human rights law. Tallinn 2.0 also explores how the general principles of international law, such as sovereignty, jurisdiction, due diligence, and the prohibition of intervention, apply in the cyber context. The document’s creation was done independently, although the NATO, International Red Cross and the United States Cyber Command were consulted as external agents for veracity. It was published by the Cambridge University Press, and was peer reviewed before its release. Tallinn 2.0 is an excellent document that should be adopted into a full treaty, rather than remain an academic paper.

**CONCLUSION**

States have the responsibility towards its citizens to account for the uses as misuses of modern technology, both by local and external agents. If a state fails to provide proper security towards a citizen, this by itself is a human rights violation; although the human rights article takes security to mean physical security, if a person’s livelihood can be threatened somehow with digital means (as seen in NotPetya), it should also be accounted for. A state exists for its people, and should protect its people from everything it can and/or it can foresee, including itself: democracy has tree powers - executive, legislative and judicial - precisely to hold the government accountable.

Mass surveillance is highly controversial and dangerous towards human rights. With the Five Eyes Alliance, states have been circumventing the law to hold them accountable and engaging in unwarranted and unmerited monitoring of citizens, in their own countries and elsewhere. While there is slim to little chance of such alliances from being stopped, the international community can and should hold these countries accountable for their actions; in 2014 Australia was ordered by the ICJ to stop spying on East Timor, which it was doing with the resources acquired with this alliance. This sort of rulings should also apply to less vulnerable countries. If anything, it is the developed countries that are at the most risk of the human rights violations with and through digital media, as these are the ones where it is more widespread used and depended upon.

New policies should be created for protection for both citizens and states in the cyberspace, old policies should be remediated to account for new scenarios, international communities should hold state actors accountable for their actions. The remediation list for the dangers of cybersecurity is long and largely unexplored, but the existing analysis and documents prove a good place to start.

**REFERENCES**

ACLU. (n.d.). *The Human Right to Privacy in the Digital Age.* From ACLU: https://www.aclu.org/other/human-right-privacy-digital-age

Amnesty International UK. (2018, October 8). *Why we're taking the UK goverment to court over mass spying.* From Amnesty International UK: https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden

Boffey, D. (2018, October 25). *UK refusal to cooperate with Belgian hacking inquiry condemned .* From The Guardian: https://www.theguardian.com/uk-news/2018/oct/25/uk-refusal-cooperate-belgian-hacking-inquiry-condemned-gchq-belgacom

Bowcott, O. (2018, September 13). *GCHQ data collection regime violated human rights, court rules.* From The Guardian: https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules

EFF. (n.d.). *NSA Spying*. From EFF: https://www.eff.org/nsa-spying

Freedom House. (2018). *The Rise of Digital Authoritarianism.* From Freedom of the Net 2018: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism

Global Internet Liberty Campaign. (n.d.). *Privacy and Human Rights: an International Survey of Privacy Laws and Practices.* From Global Internet Liberty Campaign : http://gilc.org/privacy/survey/intro.html

Gollom, M. (2013). *Are there International Rules for Cyberwarfare?* From CBC: https://www.cbc.ca/news/world/are-there-international-rules-for-cyberwarfare-1.1323638

Gomez, M. A. (2018, November). *In Cyberware, There are Some (Unspoken) Rules.* From Foreign Policy: https://foreignpolicy.com/2018/11/06/in-cyberwar-there-are-some-unspoken-rules-international-law-norms-north-korea-russia-iran-stuxnet/

Greenwald, G. M. (2013, June 11). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* From The Guardian: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Internet Governance Forum. (2018, November). IGF 2018 Chair's Summary. *Internet Governance Forum.* Paris. From Internet Governance Forum: https://www.intgovforum.org/multilingual/index.php?q=filedepot\_download/6212/1417

Internet Governance Forum. (n.d.). First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct. From https://www.un.org/press/en/2018/gadis3619.doc.htm

Jensen, E. T. (n.d.). *The Tallinn Manual 2.0: Highlights and Insights.* From Georgetown Law: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

Kimball, D. (2017, December). *The Wassenaar Arrangement at a Glance.* From Arms Control Association: https://www.armscontrol.org/factsheets/wassenaar

Mehrotra, D. (2018, February). *Net Neutrality isn't the Problem - it's the Internet Itself.* From Quartz: https://qz.com/1204956/net-neutrality-isnt-the-problem-its-the-internet-itself/

Ruiz, M. M. (2018). Bridging State-level Cybersecurity Resources. *Lawfare*. From https://www.lawfareblog.com/bridging-state-level-cybersecurity-resources

Sean McDonald, A. X. (2018, December). *The War-Torn Web.* From Foreign Policy: https://foreignpolicy.com/2018/12/19/the-war-torn-web-internet-warring-states-cyber-espionage/

United Nations. (n.d.). Universal Declaration of Human Rights.

US Legal. (n.d.). *Uniform Computer Information Transactions Act Law and Legal Definition.* From US Legal: https://definitions.uslegal.com/u/uniform-computer-information-transactions-act/

Wheeler, T. (2018, September). *In Cyberwar, there are no Rules.* From Foreign Policy: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/

Whitman, R. (2013, December). *The NSA Regularly Intercepts Laptop Shiptmens to Implant Malware, Report Says.* From Extreme Tech: http://www.extremetech.com/computing/173721-the-nsa-regularly-intercepts-laptop-shipments-to-implant-malware-report-says