This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Cyber Trends: The Gunpowder of the Twenty-First Century

https://www.e-ir.info/2023/09/09/cyber-trends-the-gunpowder-of-the-twenty-first-century/

DYMA SOSNOVSKY, SEP 9 2023

Gunpowder was invented in the ninth century in China. It was mostly used to make explosive arrows and lances until it made its first appearance in Europe in 1267, following the Mongol invasion. Over 300 years after the initial invention, it enabled the creation of weapons that would transform warfare and change the world forever. In 1453 these weapons brought down the world's longest-existing empire as the Ottomans overcame the walls of Constantinople using the Basillica gun. Fast forward to 2017 in western Ukraine and the site of one of the biggest cyber-attacks known to date – NotPetya. Originating in the Russian Federation, this piece of malware managed to infect, encrypt, and subsequently wipe thousands of devices all over the world. Events like NotPetya contribute to bigger trends. This article identifies these trends and relates them to the world of international relations. In this inspection, it is important to take into account the unique features of the cyber world as it relies very little on the physical boundaries that the field of international relations is so familiar with, making their interplay all the more interesting.

Trend 1: Increasing Global 'Attack Surface'

Attack Surface is a term cyber professionals use to define the points of contact, which can be used to perform a malicious activity. It is used when describing a system or an entire IT infrastructure of an organisation or a state. Throughout the last three decades, we have seen a dramatic increase in the 'global attack surface'. The invention of the internet together with the advancement of computers opened up an entire new world – the cyber world. Before, one state could physically send an agent to another state to gather intelligence, or an army to attempt to dramatically shift the balance of power. Now, states can hack to gather intelligence, or disrupt the national electrical grids and systems of their enemies. Before, a criminal could pickpocket you on a bus or a train. Now, they can encrypt your computer and demand a ransom.

Historically, a sudden increase in global attack surface led to a series of dramatic developments which usually also increased the rate of innovation. For example, in the late fifteenth century, the technology of navigating the oceans became accessible enough for people to sail long distances regularly. Humans gained the ability to get to other continents effectively, and the parameter that changed was precisely the global attack surface. There were more points of contact for people to affect the world around them, they were no longer limited by the confines of the land they were standing on. People started performing activities (whether malicious, or not) easier, and in more places. The result was an unprecedented rate of development, as well as the rapid expansion of some states resulting in a dramatic shift in the balance of power.

To make it more relatable to the non-physical world of cyber, the invention of the printing press is another example of the increasing global attack surface. This invention led to processes of similar magnitude. States, organisations, and private individuals became able to send information with unprecedented speed, scale, and range. The result is something we are still experiencing today – an increased capacity to exchange ideas. Some of these ideas are good for some and bad for others, meaning effective propaganda campaigns could shift the balance of power. The invention of the internet exacerbated the effect of this further.

Trend 2: Increasing Malicious Activity of Nation State Sponsored Actors

A Nation State Sponsored (NSS) actor is either a group of private individuals sponsored by a government, or a group directly representing a government. They perform cyber malicious activities, usually, by combining the use of malware with more traditional operations. In the cyber world, there are databases and classifications thereof of infinite complexity. Some NSS actors are referred to as APT's (Advanced Persistent Threats). Each new uncovered and analysed piece of malware is more complex, deceitful, and destructive than the previous one. A lot of these developments are coming from NSS actors, which indicates large interest and investment by nation states (Mitre ATT&CK Database, 2020). The last decade has observed an increase in number and scale of cyber-attacks performed by such actors (Microsoft, 2022 – see Figure 1). They do it because it leads to tangible changes in power relations.

Stuxnet is a computer virus discovered in 2010 that could target control systems of different industrial facilities (Mitre ATT&CK Database, 2020). It is believed to be responsible for causing damage to an Iranian nuclear facility by tricking its control systems into misreading the operational safety data. As a result, when such an operational hazard occurred – the rotation speed of the facility's motors did not match the intended speed – the system ignored it. This strategic facility was forced to a halt. It is understood to have been developed jointly by NSS actors from the USA and Israel, although this was never officially confirmed (The Washington Post, 2012). This might be an example of a state causing physical damage in another states critical infrastructure.

Operation 'Ghost' is attributed to APT28 and APT29. The goal of this operation was to gather political intelligence for the Russian Federation in the countries of the EU and the US, as well as influence political decisions – the outcome of elections, for example (Mitre ATT&CK Database, 2023). A combination of conventional and cyber means was used (Operation Ghost, 2019). Russian diplomats, acting as undercover agents were used to deliver spyware through USB drives, for example. They would infiltrate political institutions of the EU using the rank and the trust gained, and insert the USB drive into a relevant machine, or ask someone else with a higher level of access to do it for them. Complex malware that differed from the one used in Europe was used in the US. Taking advantage of a fewer number of cyber security laws in the US, the Russian APTs were able to use some of the cyber infrastructure in the US to host their operation to influence the elections. Russia was able to exert power through cyber means.

In 2017, the world was shocked by destructive malware that was masked to appear as ransomware. Thought to be from the 'Petya' malware family (2016), cyber experts underestimated its new variant in 2017, thinking it was another piece of ransomware. It originated in the Russian Federation and targeted Ukrainian devices, especially the government owned machines, as well as the Ukrainian energy infrastructure. This variant turned out to be a wiper attack – it erased information from infected machines (Crowdstrike Blog, 2017). It used the ransomware appearance only to mask itself and trick the defenders. The attack quickly spilled over and spread all over the world, earning a new, somewhat bitter name – 'NotPetya' (Mitre ATT&CK Database, 2018). Russia's APT28 was able to cause physical damage through cyber means.

Trend 3: Different Approaches to Cyber Legislation Around the World

Malicious activities are not the only thing that comprises the cyber world. Just like any other invention, computer technology is often used both for good and bad. However, there is a fine line between what some consider good and bad. A good example of this is the question of privacy. Privacy, among other things, is an aspect of the cyber world that many governments are attempting to regulate. Since each government views the issue differently, the legislation they erect differs dramatically. If the different states keep playing by rules (laws) that differ, they might end up in very different places in the future. Consequently, different philosophies of cyber legislation can be identified throughout the world with major powers such as the EU, the US, and China, each following their own approach.

The European multicomponent cyber security strategy, when compared to other places, can be described as strategy with security as the first and utmost priority (European Commission, 2020). I call it 'European Protectionism'. Other considerations like innovation, do not come close to the top in the European priority list. This strategy attempts to avoid malicious activity, internal or external, by limiting the means to perform it. However, limiting one thing often

has a limiting effect on other related things. For example, it is much more difficult to develop something new, or take on a risky cyber business venture in Europe than it is in the US because of more complex bureaucratic requirements. If this trend continues, the EU will not be an agenda setter in the cyber world, but rather a referee, due to its limiting strategy requiring a large number of rules that are then slowly 'exported' globally.

The regulatory landscape in the US, on the other hand, can be described as much less strict, allowing for more room for maneuver for people with ideas about how to navigate and develop the cyber world. I call it 'American Opportunism'. A recent example of this is ChatGPT. Although there were some herculean efforts put into the development of powerful generative AI elsewhere, the Americans did it first. Naturally, such a non-limiting approach comes with a cost. The cost is a systematic compromise in security. Even though, at the moment, the US takes the lead in AI and other cyber developments, the security risks that are left unchecked for long enough can, and will be exploited by the malicious actors. Either internally or externally.

As opposed to its peers, China has not yet not settled into a specific cyber legislation philosophy. Instead, we can observe China playing to its strengths in a more traditional way. The sheer size of the Chinese state and economy helps it cross-fuel the different aspects of its existence. A very high human capital produces a very high economic capital. In turn, it provides strong political capital. Together, it all fuels China's growing cyber capabilities that it uses how it pleases. There are allegations that TikTok, a Chinese-made mobile application, gathers much more user data than necessary (Forbes, 2022). How the app uses this data and who it shares it with is largely unknown – an indication of China already exercising its cyber capabilities. Although not settled into a specific cyber philosophy yet, any change in Chinese policymaking has a potential to affect the world.

It is important to remember that other parts of the world can consolidate their cyber legislation in the near future, and achieve legal parity with the above-mentioned super powers. If either the African Union or a collective of South American states manage to do it, the global dynamics of cyber legislation might change significantly from that moment onwards, and current projections may no longer apply – something that many cyber experts often fail to consider.

Trend 4: Decreasing Security, More Room for Innovations

We are governed either by the rules we come up with for ourselves, or by the rules of nature. When we did not come up with a rule for some aspect of our life, we rely our natural tendencies. One such tendency is something humans were doing for the majority of their existence – innovating more when they feel less secure. Often, one of the main blocks for innovation is the fear to compromise the already existing security structure.

Ukrainian soldiers in the Russo-Ukrainian war already showed a lot of wit and ingenuity attempting to innovate. Much of it was enabled by the relatively non-existent security environment of the war. One example of this is the implementation of 'GIS Arta' application – widely used by Ukrainians located around the frontline since 2014 (GIS Arta, 2014). It is used to gather information about enemy positions, movements, and maneuvers. The app then sends the information to the artillery regiments and helps them coordinate and correct their fire. During peace time, developing and using such an application would have been deemed very risky and insecure. After all, the enemy can hack into the app and steal the data. However, in this situation a more immediate threat than a potential compromise of the application is the enemy artillery fire. The AFU (Armed Forces of Ukraine) would much rather have a vast network of informers in real time, and occasionally deal with a cyber-attack, than not. There are many more fascinating examples of such innovation-security trade-offs being made in this war, as well as in other places around the world. To find out more, I recommend going directly to one of the many primary sources.

The world of cyber security is well described as a game of cat and mouse between attackers and defenders. There is a constant cycle of malicious actors creating new malware, as well as attack models that are then used to do harm. In turn, cyber security experts or other interested parties – the defenders – come up with new ways to mitigate or even neutralise the most recent malware, and attacks in general. After that, the cycle repeats. Zooming out and applying this cycle to a global scope highlights a dynamic in which a higher number of cyber attacks stimulates the development of a higher level cyber defences. And vice versa. Both sides are forced to innovate – the attackers

innovate to overcome the newly created defences, while the defenders innovate because of decreased security.

Trend 5: Generative AI Will Make Us Play an Old Game with New Rules

The rapid development of generative AI (Artificial Intelligence) is taking the world by a storm. Its various applications have the potential to disrupt entire industries. One such application relevant to the cyber industry is writing code. The AI makes the process of software development, malicious or not, much faster and more accessible than ever. While this is great news for a day-to-day developer, many fear that it will disrupt the global balance of power. Consider the increasing number and complexity of inter-state cyber-attacks. There is an argument to be made that, with the help of generative AI, previously unnoticeable players will be able to punch above their weight, equalising the international playfield. If smaller states are able to exercise capabilities similar to the greater state powers, the world will become more unpredictable and uncertain.

Although this may be a realistic scenario, it has one major contingency – availability of resources. Creating, training, and then maintaining advanced generative AI that is able to inflict serious damage requires a high amount of computational power. Today, developing such a model takes years. It is trained with data, and assistance of other computers. The more data you can 'feed' the model per unit of time, the faster and better your product will be. However, the computational power requires a high amount of specific resources that are used to produce the components of modern computers. Suddenly, the competition between the different AI models comes down to a very familiar competition for resources. Even though the smaller states will be able to have a respectable answer to the capabilities of the greater powers, the availability of computational power will remain a roadblock.

Conclusion

The cyber tools that we can already observe are young and relatively weak, when assessed from a historical perspective. Each of the five described trends, while distinct, also work together to combine the worlds of cyber and international relations in a language familiar to both. The recent events of the cyber world signal the fact that cyber methods will only be used more, and with more consequence, in the future. Already, cyber operations are able to shift the balance of power between states, be it in the world of intelligence or physically on the ground. If the world's cyber capabilities are to follow the trajectory that gunpowder once did, we can only expect to see many more such operations in our lifetimes.

Figure 1: NSS cyber-attacks. (Microsoft, 2022).

Dyma Sosnovsky is a strategy specialist working in cyber risk services. He holds a master's degree in Management of Innovation at the Rotterdam School of Management, and a bachelor's degree in Governance, Economics, and Development at Leiden University.