The cybersecurity impacts on geopolitics

Andrea Chiappetta, *Università degli Studi Guglielmo Marconi, Roma, Italy*

Received: May 1/2019
Accepted: May 6/2019

ABSTRACT. Cyber is the battlefield that nations, enterprises and citizens need to face in the next years. New paradigms and new threats are growing daily. During the cold war only a limited number of countries had the economic and technology capacity to build "weapons" to impose their role.The United States invented the internet, but the future of cyberspace and its leader is not yet defined. Now 29 countries have units able to provide offensive operations through cyber techniques and 49 have purchased malwares. The global connection and nature of internet, that provide itself instrument to hide who is behind an attack and determine whom to punish, will leave several questions open. This paper tries to provide an overview of these issues leaving some questions open to government and institutions.

KEYWORDS: *Cyber crime, cyber security, cyber warfare geopolitics, economy, international relations*

Introduction

The advancements in information technology along with growth in internet capabilities have played a vital role in the society through enhanced e-commerce, communications, data storage, digital marketing, information vulnerability. As already said, cyberspace and crime have taken a vital part in international relations, interrupting businesses while creating conflicts and tensions among different governments. Various activities have indicated that the level of the victims to cybercrimes does not matter to the cybercriminals, with governments and organizations all targeted in a spate of attacks and still remain at risk of being attacked again. The latest role played by the cyber-attacks as a weapon in international rivalries has formulated a new battlefield in the world geopolitical landscape. On this note, it is good to examine the cybersecurity of the world geopolitical landscape and what governments and companies need to do in order to prevent such attacks from hitting and affecting them in a number of ways (Kallberg, 2013).

Between the years 2011 and 2013, there were attacks on American banks, with even the New York Dam Control System being a victim if a DDoS attack executed from Iran. However, when the US decided to hold negotiations in regards to bringing an end to sanctions held against Iran with the exchange that it abolished its nuclear weapons, the attacked stopped. Nevertheless, the US has created policies that threaten the deal made by Iran and such attacks could be witnessed very soon, as retaliatory attacks begin (Maréchal, 2017).

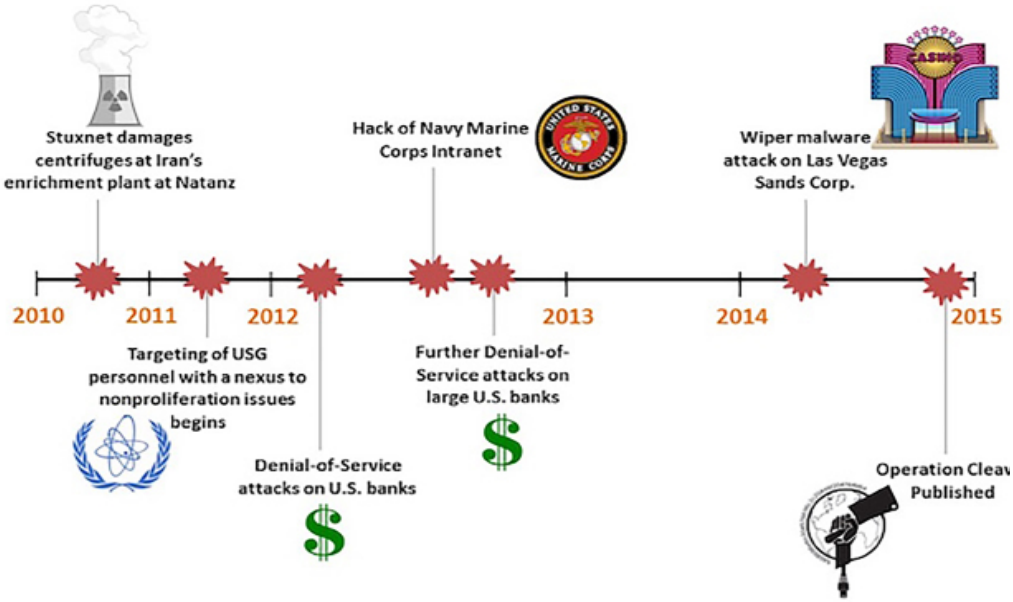

Figure 1. Alleged Iranian cyber-attacks against US Institutions

One of the greatest event in geopolitics and cybercrime is when Edward Snowden, a contractor from NSA stated that NSA, in 2013, had used metadata as well as interception of telephone messages and calls to spy on organizations and individuals, with American citizens not spared along with foreign leaders (Maréchal, 2017). The turn of events created bad blood between the US and some of the countries that were considered their biggest allies back then. Whereas all that was done under the excuse of trying to fight terrorism and ensuring the safety of the people, the foreign partners to America were not happy. Some of the countries like Brazil and Germany went a step ahead to present a unified declaration at the UN to condemn such acts from the United States of America (Kallberg, 2013).

As cyber warfare has been intensifying, it is hard to directly connect a country with certain groups of hackers, who might be or not be 'hacktivists' operating independently. The 2016 US elections witnessed one of the most hotly contested elections in the US, with Russia being accused of interfering with the title race to the US presidency. The prosecutors handling the case believed that a hacker group called Fancy Bear was the one behind the release of vital and sensitive emails for staff in the Hillary Clinton campaign and were used to spread propaganda on social media (Jensen et al., 2019). However, Russia has refuted any claims linking them to the attacks but stated, at the same time, that there was a possibility of 'patriotic attackers' acting independently. That could have tried to influence results of the elections while responding to vital international events (the tension in Syria and Ukraine). In response to that, the US has taken the initiative of banning software products from Russia like Kaspersky software and Huawei's (a Chinese company) from entering the US as there are fears that they could contain secret software that could create software loopholes within the US systems and make the country vulnerable to attacks.

International business cyber attacks

When it comes to cyber-attacks at an international level, businesses are also at risk of being attacked. The most common example is when Sony Pictures was attacked by people backed and sponsored by North Korea. This happened after Sony wanted to make a satirical movie about the North Korean leader and the news reached North Korea before the movie could be released (Kallberg, 2013). The attack was serious and made Sony go offline for some time. After the attackers got out from the system, nearly all of the information in the company's servers was stolen and ¾ of their servers were destroyed in the process. Whereas it is known that a hacker group called Guardians of Peace claimed responsibility on the attack, the initial threat for a massive retaliation action had been carried out by the government of North Korea. Eventually, Sony made a decision to eradicate their plans to release the movie, as they feared more attacks from either terrorists or cybercriminals (Bremmer, Gordon, 2011).

The latest trends in the the discovery of Blockchain technology show an international cryptocurrency phase unleased, which has been revolutionizing the way money is exchanged across borders. Many opponents of the idea argue that it is a threat to the existing traditional banking systems, eliminating the transfers of funds between banks along with the fees associated with them. The application of peer-to-peer decentralized storage of data to eliminate all traditional middlemen in international finance has created a lot of admiration for different stakeholders (Maréchal, 2017).

Despite the progress and success of digital currency being witnessed around the world, they have been unable to fully replace the traditional banking and money transfer system. The main reason why digital currencies did not manage to replace banks is cybersecurity. Many accounts have been hacked in some of the most renowned platforms such as Coinbase. That caused great losses, and likewise made the initial investors into cryptocurrency (e.g. Ethereum, Bitcoin) to lose their faith in that. Digital wallets have been considered to be unsafe to keep large amounts of digital currency. The biggest issue is that once someone loses his or her wallet details, all the funds associated with the wallet are lost (Kallberg, 2013).

When a cryptocurrency mining pool gets more and more stake in the distribution chart of hashrate, they go against the decentralization purpose. When a section of miners control majority of hashrate, they become the main players. In many cases, if the miners control 51% of the hashrate in the network, they initiate an attack renowned as "the 51% attacks".

The 51% attack takes place when a total of 51% of hasrate in the network is under a single entity. The entity could be a pool of miners or a figure with authority. At the time the 51% of the hashrate will be sieged, it actually destroys the decentralized form and opens up the network to the following attacks:

a. Selfish mining
b. Double spending
c. Cancelling all transactions
d. Random forks

The most common type of 51% attacks can take place when a pool of mining tends to be too large and goes beyond the 51% hashrate. It has already taken place with bitcoin at some point. On July of the year 2014, the renowned mining pool by the name GHash.io went above the 51% hashrate. After that, they voluntarily reduced their hashrate and promised that they would never go above 51%.

The attack was also instigated on Shift and Krypton, which are Ethereum based Blockchain. Smart contracts have been introduced in cryptocurrencies to make work easier. Here, through the format, the contracts are converted into computer code, stored and duplicated within the system and maintained by a network of computers which operate the Blockchain. This also leads to a ledger feedback like transferring money and getting the service or product. Cryptocurrency mining has been of the main weak points that hackers capitalize in to attack people's wallets. The trend has been on the rise, as hackers have created new ransomware with advanced capabilities to attack the digital currency. Data obtained from Kaspersky Labs show that in 2017 the number of Trojan horse attacks on cryptocurrencies was more than 1.65 million. The trends are presented in the graph below:

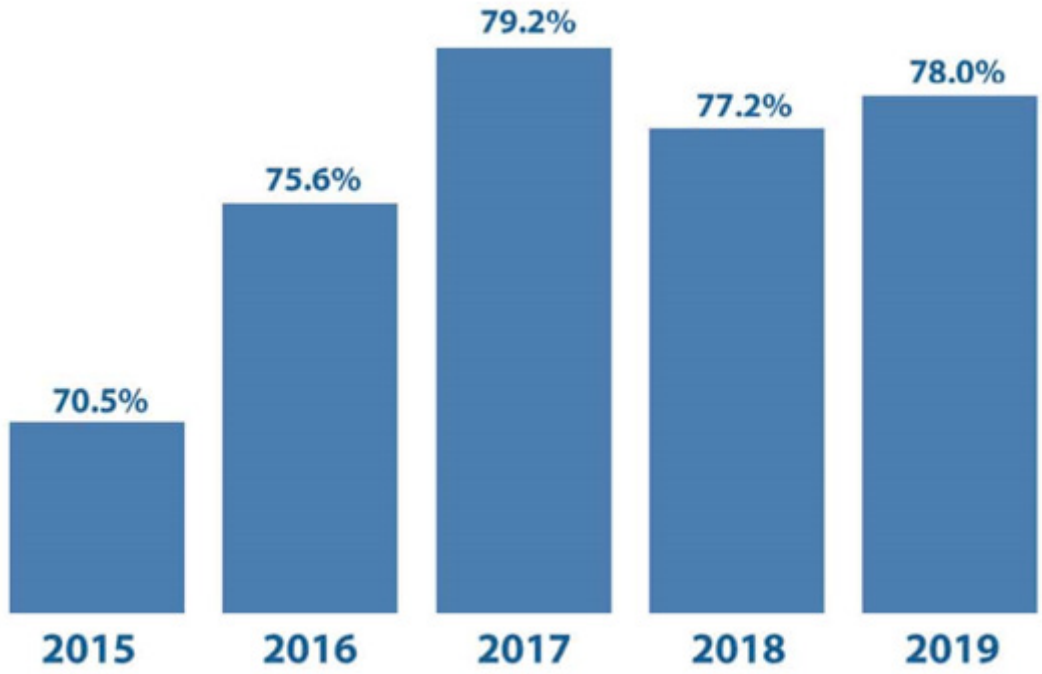

Figure 3. Cyberspace attacks on digital currencies around the world

Cyber as a war theatre

Even if there is a lack of recognition cyber-attacks at a national level, there is no doubt that cyber warfare has been around, is ongoing and will continue in the future. Various governments are showing reluctance to acknowledge openly the reality, because they fear that such a recognition will need retaliation. Moreover, a greater fear is that it could trigger a kinetic warfare. In any case, having kinetic provocation translates to kinetic responses, but cyber provocation does not tend to consider that. For instance, there were different viewpoints on the attack by the US to respond to the missile tests in North Korea as compared to when North Korea attacked Sony pictures and SWIFT (Maréchal, 2017).

Throughout history, it has been seen that each time there is a new invention and new weapons always give an edge to a country over others at a time.

That has encouraged the countries to pursue more expansion of their dominance at an international level. For example, as soon as the US created nuclear weapons, it hastily tested them on innocent people of Nagasaki and Hiroshima in the final stages of World War II. The tests led to enormous ecstasy among the Elite in America, who then started plotting to attack the USSR and take back into the Stone Age. Nevertheless, at that moment, the US had created enough nuclear weapons to attack and destroy USSR, whereas Moscow had created its own nuclear weapons to retaliate in case it was attacked. That helped Russia escape the attack that could have taken the country so many steps behind (Maréchal, 2017).

Over the recent past, the great possibilities and capabilities of the internet and different cyber platforms allowed the US to take down different countries while pursuing their own policies and used "color revolutions". Such interferences led to the whole Middle East to get into political and international chaos, which formed preconditions for many armed conflicts in which people died in the process. In the end, NATO allies benefitted more from such conflicts, as they supplied weapons to the warring nations.

In the modern-day world, the latest advancements in IT together with new technological inventions in the areas of chemical, space, and biological warfare are now leading to unbalanced fantasies of the strategists from the American Military. According to many researchers and analysts, the future wars will not be concentrated on bombs and bullets but mostly on the internet. Hackers currently have the capability of destroying any hydroelectric power plant, control system or even nuclear reactors. Thus, having like 19 hackers can lead to greater damage than the famous 19 terrorists who hijacked civilian jets back in the year 2001, when the most terrifying attack in the US history happened (Jellenc, 2012).

The global security community knows that the current cyber era has conflicts that are resolved and fought without any formal regulations or rules. Each country has the ability to invest in developing cyber capabilities. Because of the nature of technologies that are currently being used, each country has the capability of using it without being noticed, causing very serious damages over time. In February 2014, President XI said that without cybersecurity there is no real national security.

As normally is the case, it is the common people who are the greatest victims of such silent cyber-attacks. The major factors which expose people to such attacks include:

a. Large-scale diffusion of communication and computer networks
b. Vulnerable and unmanaged interconnections between vital systems
c. Rapid changes in the landscape of technology
d. Inexistence of cyberspace boundaries

From the perspective of regulations, it is vital to offer the responses provided below:

a. What could be the effects of using force in cyberspace?
b. At what point should cybercrime deemed as an armed attack?
c. What techniques and levels of balanced responses should be used against attacks?
d. What are the set of rules to be applied to making such a type of response to attacks?
e. How can one establish the legal liability of the actors entangled in cyber operations?
f. How is it possible to formulate balanced international security needs with the vital need to protect citizens' individual freedom?

Economic data and strengthening of international cyber capabilities

Currently, there are several projects being run by governments to help them have an extra edge in terms of cybersecurity. One of the most recognized projects is Plan X (Cole, 2017), which is an initiative of the US governments, that is being developed by the DARPA division, in order to implement new technologies for cyber warfare. In addition, other ongoing projects are financed by the United States. For instance, the AFRL (Air Force Research Laboratory) contracted six firms (using over $300 million) under the ACT program to offer cyber weapons on-demand under a contracting form called IDIQ. Nevertheless, such projects are top secrets for the government and there is little information available about them. There is no information on the existence of similar projects being carried out by nations like China and Russia, although such projects could be done in the background without letting the public know, because the aspect lacks transparency at many levels (Cole, 2017). The Armed forces of Russia announced a national requirement in developing and regulating cyber weapons, and the PLA of China is taken to be one of the heaviest investors in cyber warfare. Also, considerable efforts have been made by countries like Iran and the UK to form cyber warfare weapons.

In the recent past, other countries made confirmation that they will be engaged in the new domain and create their strengths in cyberspace. The ministry of defense in Scandinavia intends to create exploits and malware to start counter-attacking any threats that come in their way.

At the same time, Taiwan is making heavy investments on the new cyber warfare abilities along with NATO, in order to boost its defense capabilities. Starting the year 2012, NATO spent a total of 58 million USD (Lacy, Prince, 2018).

The table below shows expenditures by some of the key nations in enhancing their cyber warfare capabilities (Dalby, 2017).

Country	Year	Project	Amount (millions)
NATO	2012	Cyber defense capabilities upgrades and enhance the NCIRC (NATO Computer Incident Response Capability) to attain full operational capabilities by the end of the year 2012.	€58
US	2013-2017	DARPA was assigned a budget of $1.54 billion to run from 2013 to 2017 to emphasize on increasing cyber-offense to achieve the needs of their military.	$1540

Table 1. Regional and country expenditures on enhancing cyber warfare capabilities

The global cyber warfare market

The market size as per the year 2016 was estimated to be at USD 20.10 billion, showing an 18.5% CAGR over the period of forecast. Over the recent few years, the different governments and international companies have put their emphasis and focus on cybersecurity because of the increased challenges brought within the cyberspace. The issue has raised alarm and concerns in different international security agencies, thus creating awareness and readiness to boost cybersecurity. Therefore, the military, governments as well as other agencies have been involved in ensuring that they protect their infrastructure as well as connected devices from any possible cyber-attacks (Cole, 2017). Increased expenditures to improve the effectiveness of governments, their efficiency as well as boosting their capabilities in cybersecurity is expected to be a vital factor in enhancing the implementation of systems of cyber warfare across various geographic regions. The main aims of modernizing the IT infrastructure across different governments, boosting deteriorated facilities as well as reducing cyber vulnerabilities, are still on course and expected to drive the market over the time it is being forecasted. Countries like the US have taken the aspect of spending on cybersecurity with a lot of seriousness and have spent a lot over the past few years. The table below - Grand Review Research, 2018 - shows the cyber warfare market in the US by application forecast from the year 2014 to 2025 (USD billion).

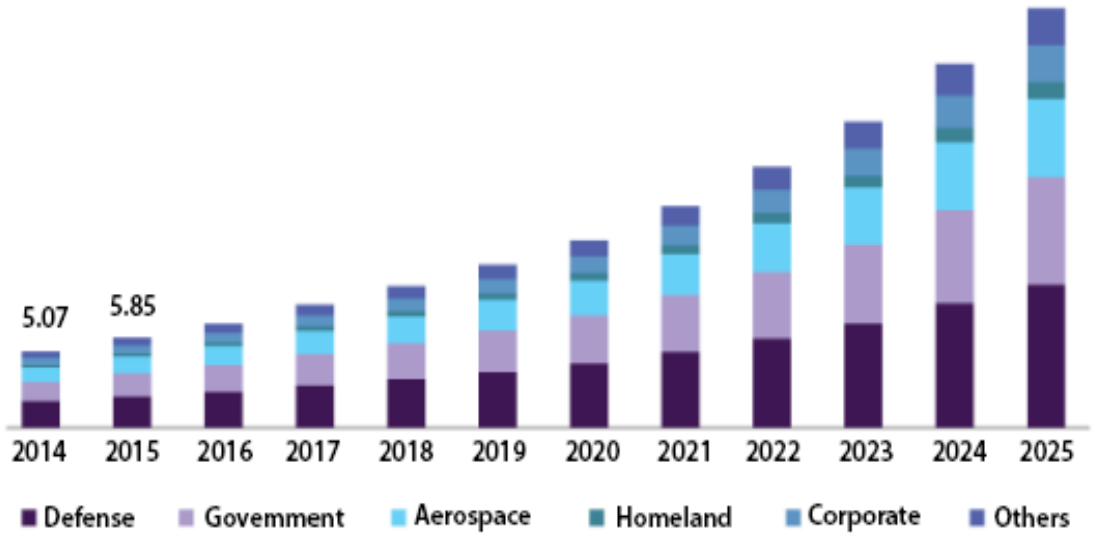

Figure 4. U.S Cyber warfare market, by the application (2014-2025) in USD billions

The increasing developments in information technology and the capabilities of cyber weapons have led to many countries to witness their national securities disrupted on a constant basis, which has, in turn, reshaped the landscape of threats. Therefore, cyber-related threats have been pointed out as one of the greatest global risks now. At the same time, cyber warfare represents a considerable threat to different countries, even posing a more serious threat than terrorism. Loss mitigation came up because of the increased cyber-attacks in various nations, leading to economic disruption (Lacy, Prince, 2018). As developing nations warm up to the phenomenon of digitization, cyber warfare has become a

constraint to their growth. For them to avoid cyber spying and breaches of data in their military and the sector of defense, various countries have added on their spending on cybersecurity and have also created units solely involved in overcoming the challenges of cybersecurity. Therefore, enhancing the demand for cybersecurity is expected to drive the market over the period of forecast between 2014 and 2025 (Lacy, Prince, 2018).

For some years now, different industries have seen a steady rise in the number of breaches in security that have been connected to cyber spying. The complexity of cyber attacks has increased and state hackers have the power to abuse the network security and get privileged access to some of the most sensitive data in the network. For example, in the year 2017, the ASD (Australian Signals Directorate) made reports of breaches to very sensitive and high-level information like the warplanes of Australia and Navy ships that were stolen from a Defense subcontractor in Adelaide. The mysterious hacker called *ATP ALF* took information on programs like the F-35 Joint Strike Fighter project, C-130 Hercules transport plane as well as the P-8 Poseidon maritime surveillance aircraft project. The hacker also successfully accessed the system for one full month before he was detected in November 2016 (Lacy, Prince, 2018).

The Federal Government of the United States has taken many initiatives against cyber-attacks and has always shown its capabilities in cyber warfare to help deal with complex attacks. The US government is also building its cyber army and, in fact, it has a total of 133 teams in place to ensure it has enough cyber arsenal by the year 2027. To ensure that, the government takes part in proactive development and training to the personnel in the military to ensure enough promptness and ability to combat cyber-attacks and initiate some when the need arises.

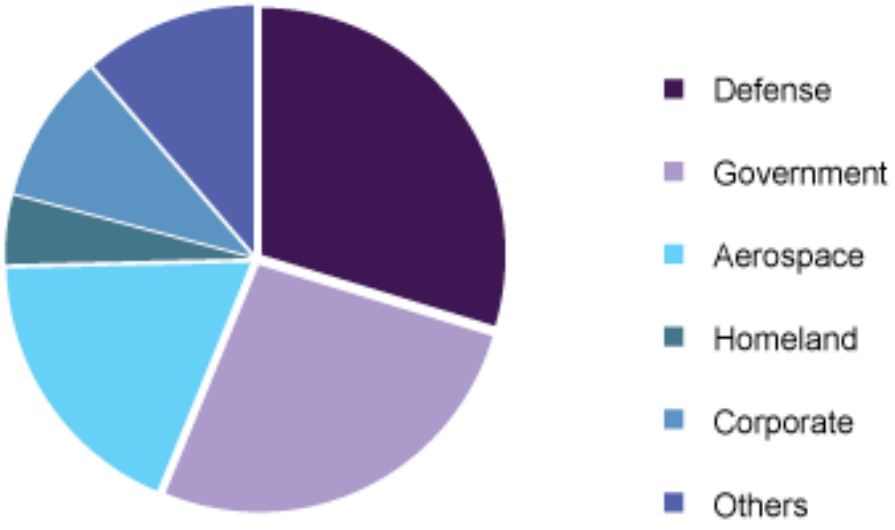

Figure 5. The global cyber warfare market share by the application in the year 2016
(Source: Grand Review Research, 2018)

Increasing international coordination in cybersecurity and adaptation of

cyber norms

ICT (Information and Communications Technology) brings one of the latest challenges in global security. Assessments on threats indicate that the next biggest international crisis could come as a result of terrorist or state group making ICT weapons that would be devastating to the critical infrastructure or networks of military logistics (Fitton et al., 2015). The explosion of asymmetric warfare (conflicting nations or groups with different military abilities) has enhanced how states use ICTs, which has necessitated the nations to develop an international cyber conduct code (Jellenc, 2012).

There exists urgent need to have the nations cooperating to reduce or deal with the threats like cyber attacks, cybercrime, electronic spying, offensive operations, and bulk data interception with an aim of using them to their advantage and compromise international security. The latest emerging cyber threats could take part in massive societal and economic damage and sabotage, thus creating the need for international action to recalibrate and deal with the new reality (Guiora, 2017).

There is a common misconception that the main threats in cybersecurity needing international collaboration are great, state-sponsored attacks which are aimed at critical infrastructure like power plants on electrical grids, leading to human casualties and massive devastation (Deibert, 2015). To be precise, cyber threats are different and complex, mostly targeting private companies as well as endangering the digital world's technical integrity. The business models of near-total digitization make the world economy to be more vulnerable to cyber-attacks, from both criminal organizations and fellow states and non-state actors.

The following graph presents some of the global cyber incidents that have affected different nations (Dewar, 2014).

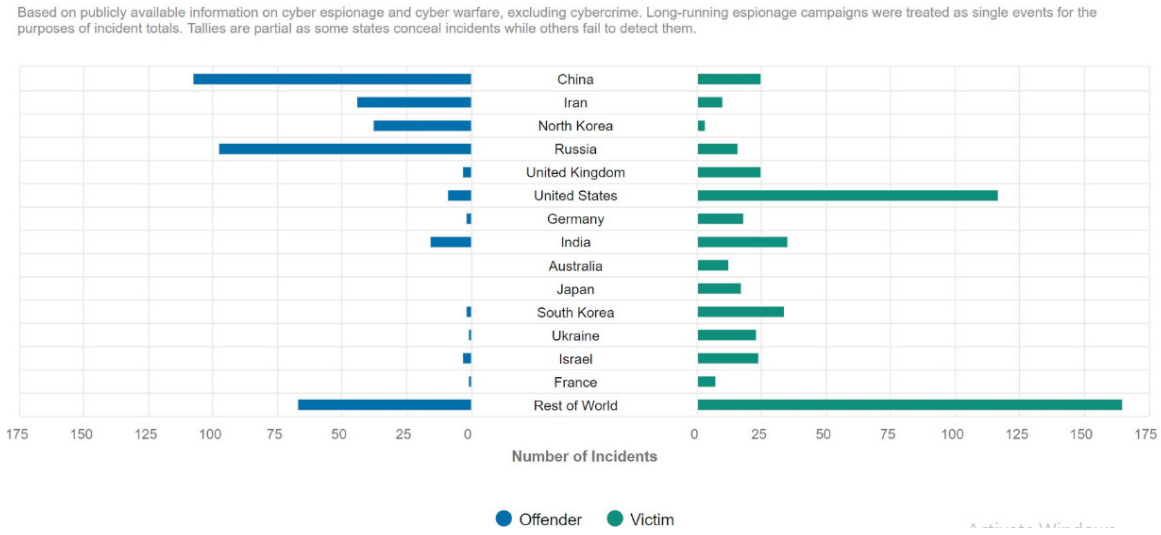

Figure 6. Significant international cybercrime incidents (Source: Dalby, 2017)

The latest legislation like the European Parliament's directive on the security of network and information systems considered the aspect of state-managed attacks into account (Aggarwal, Reddie, 2018). The European Parliament's directive, whose focus is broadly on the threats to vital infrastructure, intended to enhance measures of cybersecurity towards safeguarding the basic services like search engines, market places, as well as cloud computing mainly applied by citizens, governments and citizens. Having any major disruption of such services might be destructive to the existing business models and create a lot of losses in the business' operations (Guiora, 2017). There are many sectors targeted by such geopolitical cyber-attacks. Governments and corporates are being targeted on a daily basis. Sectors such as power and utilities, petroleum, transportation, water, food and beverage, chemical and different others (Dewar, 2014). The power and utilities are the most targeted because they are believed to be pivotal to the management of economies around the world. The petroleum and transportation industries are the second targeted sectors by international hackers, as they intend to cripple the economies of their target countries (Deibert, 2015). The graph below presents the most targeted industries around the world by international hackers:

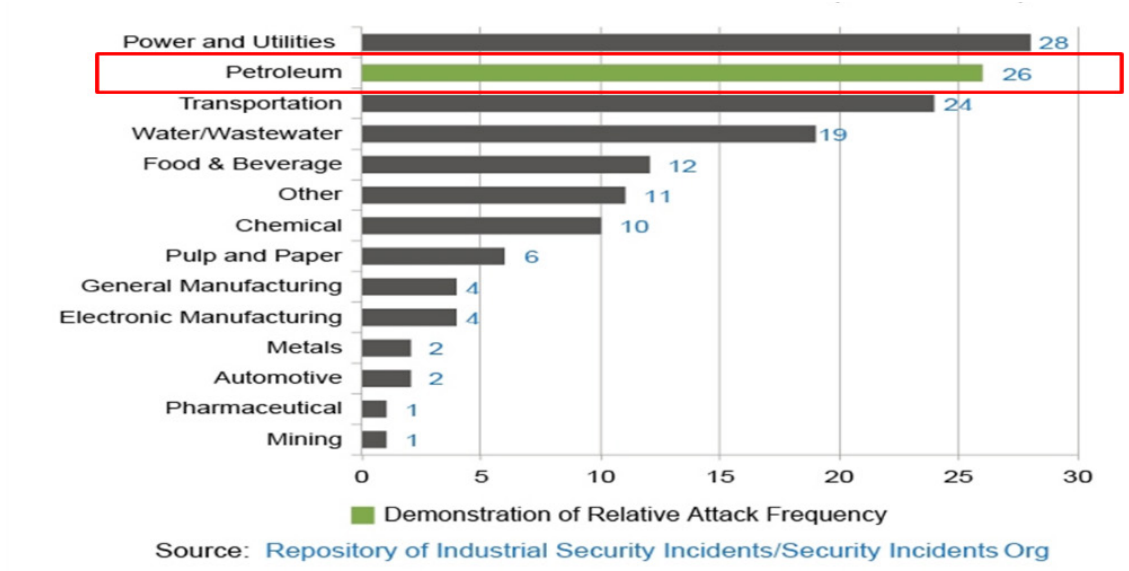

Figure 7. The most targeted Industries (Global) (Source: Dalby, 2017)

In May 2017, there was a series of attacks by cybercriminals through the use of WannaCry ransomware, which affected several computers around the world. The attack cost the affected parties a total of $1 billion. However, the UK, US, and other nations connected the attack to North Korea. After WannaCry, another wiper-malware (NotPetya/Petya) attack destroyed records from the systems that had been targeted without demanding or collecting any ransomware. The short-term but large-scale outbreak linked to a state actor had effects on several companies across the globe and had been estimated to cost the Maersk a total of $300 million that they lost (Chernenko, 2018). The future looks quite uncertain, but it is clear that cyberspace will be the major focus of governments. Strong economies like the UK and USA have invested a lot in cybersecurity. Thus, it is expected that governments will be run using the internet and their strength will be measured by how much power they have in their cyber systems. Weapons will be used, but the ability to control the weapons using computers will be the key feature in the future.

Recommendations for future actions

a. **Create an international cyber court**
Because of the increasing number of accusations on cyber attacks among different countries and the complexity of technical attribution, it could be advisable to formulate an international court that is independent or formulate a method that will only deal with government-level cyber conflicts and that could be considered and respected by all parties involved (Guiora, 2017). In a court like that, one of the parties could bring their evidence that they were hacked, then the accused party could be given a chance to argue for or against the attacks with opinions given by experts. Such an approach would be important in settling down the current wrangles between the US and Russia which started in the 2016 US general election (Chernenko, 2018).

b. **Restricting autonomous cyber weapons**
Cyber weapons, which are automatically operated without human participation such as the US Project Monstermind, should be banned and outlawed. Normally, attacks are routed through computers in innocent developing nations and put at risk citizens' information, from such countries, with autonomous cyber weapons which do not have any rules on national borders or humanity. The CGE and UN meeting held to discuss lethal weapon systems in the year 2017 was the only first formal meeting in which such weapons were discussed (Chernenko, 2018).

c. **Codifying the cyber attack legislation into an international law**
The long-term goal for the international bodies should be signing a binding convention under the UN to fight cybercrime, as well as create a universal code of conduct for countries in the cyberspace. The recommendations of the UN GGE have already in place can be used as the starting point of the code (Chernenko, 2018).

d. **Using Internet of things to connect**
Internet of things is a new phenomenon that has come up and it has helped connect different people, businesses and machines. Through IoT, cyberattacks will be reduced because systems will be interconnected and detecting attacks will be easier. By the year 2020, it is anticipated that a total of 28 million devices will be connected through IoT However, this might present a security threat as well because attackers will easily find loopholes to attack different places and things that they would not have been able to.

Conclusion

Geopolitics and cybercrime have become a subject of intense international scrutiny as different countries have accused one another of hacking and interfering with one another's operations and military secrets. This has created enmity, although it all ends online as countries try to outdo one another through counter attacks. Developed nations have weaponized their cyberspace and made it ready to attack whenever they are attacked. However, if not well-regulated, cyberspace can be very damaging to different economies around the world.

Thus, it is recommended that nations come together to formulate laws and governing bodies control the use of cyberweapons among the member states. There are some proposals that can be used to increase international coordination in the cyberspace and protect the resiliency and stability of the world digital economy. There is currently no universally created body that works towards enhancing world cooperation in dealing with cybercrime and no clear mechanism to be used in developing strong believes and good behavior of countries in the cyberspace. The lack of policy enables malicious actors to use the internet in whichever way they want, without any consequences. The world needs to be safer now and not wait for a major attack to wake up and act.

References

Aggarwal Varindeer K., Reddie Andrew W. (2018), *Comparative industrial policy and cybersecurity: a framework for analysis,* "Journal of Cyber Policy", V.3, N. 3, 291-305
https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1553989?journalCode=rcyb20

Alatalu Siim (2016), *NATO's new cyber domain challenge. International Conference on Cyber Conflict (CyCon U.S.)*, pp. 1-8
https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7836073

Bremmer Ian, Gordon David (2011), *The geopolitics of cybersecurity*, "Foreign Policy", January 12
https://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity/

Bronk Christopher (2014), *Hacks on gas: Energy, cybersecurity, and US defense*
https://scholarship.rice.edu/handle/1911/91294

Chernenko Elena (2018), *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*
https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Cole Morgan (2017), *Army turns to Plan X to defend against cyber threats* https://defensesystems.com/articles/2017/09/20/army-cyber-defense-darpa-plan-x.aspx

Dalby Chris (2017), *Cyber insurance for oil companies*
https://www.eniday.com/en/sparks_en/cyber-insurance-for-oil-companies/

Deibert Ron (2015), *The geopolitics of cyberspace after Snowden*, "Current History", 114 (768), 9

Dewar R. S. (2014), *The "triptych of cybersecurity": A classification of active cyber defense*. Proceedings of the 6th International Conference on Cyber Conflict, Tallinn, Estonia, pp. 7-21

Fitton Olivet, Prince Daniel, Germond Basil, and Lacy Mark (2015), *The future of maritime cyber security,* Lancaster University
http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf

Grand Review Research (2018), *Cyber Warfare Market Size & Trend Analysis Report by Application* (Defense, Government, Aerospace, Homeland, Corporate), By Region And Segment Forecasts, 2018 – 2025
https://www.grandviewresearch.com/industry-analysis/cyber-warfare-market

Guiora Amos N. (2017), *Cybersecurity: Geopolitics, Law, and Policy*, London, Routledge

Jellenc E. (2012, July), *Explaining politico-strategic cybersecurity: The feasibility of applying arms race theory*. *Proceedings of the 11th European Conference on Information Warfare and Security*, pp. 151-162

Jensen Benjamin, Valeriano Brandon, Maness Ryan (2019), *Fancy bears and digital trolls: Cyber strategy with a Russian twist*, "Journal of Strategic Studies", pp.1-23
https://www.researchgate.net/publication/330292030_Fancy_bears_and_digital_trolls_Cyber_strategy_with_a_Russian_twist

Kallberg Jan (2013), *Cyber Operations - Bridging from Concept to Cyber Superiority*
https://works.bepress.com/jan_kallberg/1/

Lacy Mark, Prince Daniel (2018), *Securitization and the global politics of cybersecurity*, "Global Discourse", 8, N.1
https://www.tandfonline.com/doi/abs/10.1080/23269995.2017.1415082

Maréchal Nathalie (2017), *Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy*, "Media and Communication", V. 5, N.1, pp. 29-41
https://www.cogitatiopress.com/mediaandcommunication/article/view/808