ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ

CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Geopolitical Cyber Perspectives

Dragan Vitorovic

Research Paper No. 10

ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Geopolitical Cyber Perspectives

Dragan Vitorovic

Analyst KEDISA

Research Paper No. 10

Geopolitical Cyber Perspectives

By Dragan Vitorovic, Analyst KEDISA

Introduction

Most people have their existence firmly anchored in postindustrial societies, structured by the exponential growth of technology. In those societies data is gradually recombined to form a new currency. Debates on the state of AI, possible existential threats coming from technology, reshaped landscape of economy are merely some of the hot topics, continuously reaching the public on every continent. [1]
Society is moving from purely physical dimension towards a more digitized environment. Cyberworld, having Internet at its core, is vast and powerful.

This brief analysis will attempt to explain what the role of Dark Web in the current economic state of affairs is. Additionally, it will try to show whether crime also has a modified dimension within the cyberspace.

Finally, the inquiry will be directed towards the issues of how states behave in the cyberworld and what their capability in this domain may be, given the interconnected world and a new form of old challenges: how to design the regulatory framework for cyberspace.

Dark Web and Cybercrime

The news that AlphaBay and Hansa Markets have been shut down, after years of investigation led by officials from United States, the United Kingdom, Canada, the Netherlands, Thailand, France and other countries, have reached the public on 20th of July [2]. AphaBay and Hansa were the first and the third largest online markets, respectively, to deal in illegal goods such as drugs, weapons and stolen credit cards, using infrastructure of dark-web. Compared to the infamous Silk Road, shut down by the authorities in 2013, which recorded a stable daily turnover between 300 and 500 thousand US dollars, AlphaBay's daily turnover was double this amount, ranging from 600 to 800 thousand US dollars. [3]

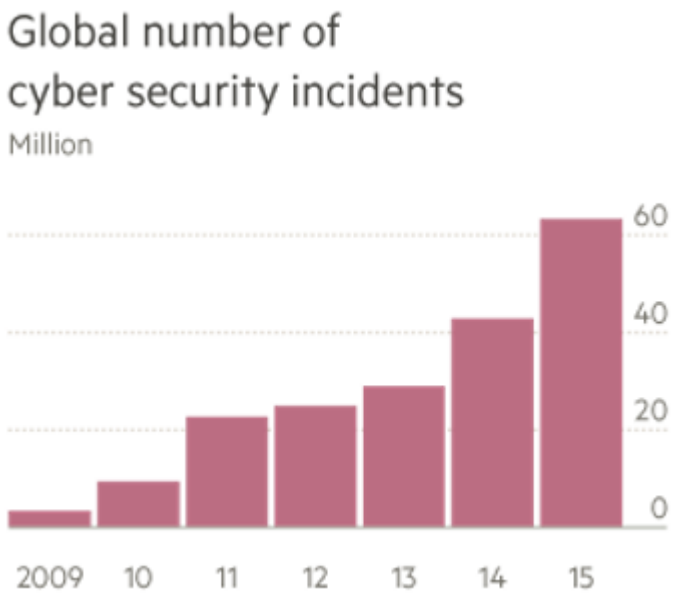
Speaking in numbers, the projected value of extracted data of European customers will reach €1tn in 2020, whereas the global cost of overall cybercrime level is expected to rise to 2tn USD in the following two years. At this moment, only ten nations have Gross Domestic Product which is equal or higher than this level, according to World Bank data. [4]

As a response to this type of activities, in 2020, business entities will invest 101.6 US billion in cybersecurity infrastructure and services, following the reports of International Data Corporation and CFA Institute. [4] Steady and persistent increase in the number of cyber security incidents, involving both state and non-state actors can be seen on the Diagram below. [5]

Following this phenomenon, Dimitris Avramopolous, European Commissioner for Migration, Home Affairs and Citizenship, suggests that the Dark Web is becoming the safe house of rampant criminality, insisting that the unlawful markets pose a serious threat for society. [6]

Given the cat and mouse game between the markets situated on Dark Web and law enforcement, the strategy for shutting such markets down may be less effective than desired, as stated in the research paper of Soska and Christin (2015). Since those markets are resilient, efficient and demand-led, and, arguably, it would be more efficient to design a strategy that could lead to decrease in overall demand. [7]

Markets on Dark Web and cybercrime, however, are not the most pressing issues when considering cyberspace.



(Diagram 1: Global number of cybersecurity incidents)

The Return of Geopolitics: Cyber Geopolitics

Given the magnitude of cybercrime, what would be the projection and the role of the state power within the cyberspace?

Combining the established dynamic feedback relationship between the technology and societal norms with the return of geopolitical considerations, would it be possible to capture the interplay between the physical and cyber worlds? Since Internet has no borders and no geography, as outlines Mikko Hypponen, this opens various possibilities for the policy-making modalities. [8]

Under the given circumstances, the space for geopolitical dynamics is finite. Every action influences and creates a response, particularly in conflict, and it would not be possible to export conflict without retaliation.

In contrast to the psychical world, cyberspace is infinite. It has its own momentum. Being much greater than Internet, yet having the Internet as its central component, cyberspace may display the similar dynamics and trigger a chain reaction as in psychical field, involving both state and non-state actors. [9] From the strategic and policy-making perspective, this is particularly important characteristic.

Surprisingly or not, states appear to be highly capable of following and shaping the cyberworld, having both offensive and defensive cyber capabilities. Through the innovation and technology harnessing, states are shaping the behavior of citizens and stakeholders, whereas cyber capabilities represent an increasingly used tool of statecraft. According to IHS Jane's, more than 100 militaries world-wide are developing cyber units, and the strategy of each one reflects the world-view approach to its state policy. [10]
As a result, state-sponsored cyberattacks have increased by 140% over the past three years, while events designed/conducted by activist and hacktivist have risen by 83%, according to findings from The Global State of Information Security Survey in 2017. In other words, states are already conducting the cyber-arms race, which may require less funding than the conventional armament, given that cyber weapons are cheap, accessible and, not to forget their important feature, deniable. [9]

As stated in the report of World Economic Forum, cyber superpowers which have responded to a rapidly growing number of attacks in recent years, heightening thus the geopolitical tensions, include the United States, China, Russia, Israel, the United Kingdom, Iran and North Korea. It is interesting that each of the nations mentioned is also in possession of nuclear programs. [11]

The Regulation Issue and the Cyber Arms Race

Similarly as in financial industry, the matter of cyberspace regulation may become the most controversial international subject. Given the devastating potential of cyberweapons and differing perspectives, it is necessary to design a level playing field for the entire international community.

The position of the European Union, and perhaps to a lesser extent of the USA, is clear: the international law applies in cyberspace. However, other cyberpowers adhere to different doctrines, particularly considering the prospects of cyberspace militarization, often disputing the concept of state sovereignty treatment in cyberspace [12].

The recent paper of Independent Commission on Multilateralism, "The Impact of New Technologies on Peace, Security, and Development" mentions that in 1998

Russia proposed a treaty on cyberweapons, similar to the one about the treatment of nuclear, chemical and biological weapons, yet it did not receive significant international support [13].

Nevertheless, changes in the world political scene have somewhat modified the stances of Russia about cyberattacks, leaving enough space for vague interpretations of international law when considering the cyberspace. Namely, Russia's Information Security Doctrine does not provide specificities on whether the norms and principles of international law apply to cyberspace, despite recognizing the international law as the guidepost of the document. Moreover, China's International Strategy of Cooperation on Cyberspace provides unclear interpretations of the international law application. Regarding the approach of NATO to this sensitive matter, the comprehensive Tallinn Manual 2.0 can be described as the guidelines followed by 28 members of Alliance.

Besides the differences in doctrines and the interpretation of international norms, blurring motifs, unclear strategic objectives and undefined adversaries in cyberworld are additionally complicating the applicability of international law. Specifically, it is very difficult to provide a viable definition making the essential distinction between the acts of cyberterrorism and cybercrime. [14]

In supporting this view, it would be useful to mention the writings of Klimburg (2011) outlining the Russian stance that the isolation of cyberterrorism and cybercrime from the concept of international information security is not the optimal policy choice. Firstly, it may lead to false understanding of reasoning behind any move related to cyberattacks, and secondly, it can result in misconstruction of the source from which the attack originates. [15] Besides, it may often be impossible to make a distinction between cyber espionage and covert action carried out through cyber means, as well as to differentiate between the preparations for cyber disruption and broader efforts in preparation for war. [16]

Conclusion

While the numbers presented in the cases of Dark Web and cybercrime activities are very high, the philosophy and approaches of cyber considerations in geopolitical

terms are much more far-reaching and important, even attempting to reframe the international norms and stances.

Additionally, the activities in cyberspace have already spilled over into the very psychical world, meaning into the hardware and the infrastructure of serious industrial and strategic potential of another nation. Perhaps the most prominent examples include the impact on Iran's enrichment centrifuge structure within the nuclear posts, using a highly-sophisticated malware, STUXnet, and the attack on Ukrainian power-grid infrastructure.

Asked to comment on whether the cyberattack on Iran was an act of war, general Hayden, former NSA and CIA high official, stressed that this can be explained as covert operation and not an act of war. [17]

Obviously, the issue of cyberspace regulation will represent a serious challenge during this and the following decade.

Bibliography

1. **A. McAfee, E. Brynjolfsson.** *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.* s.l. : W.W. Norton & Company, 2016.

2. **Greenberg, A.** Global Police Spring a Trap on Thousands of Dark Web Users. *Wired.* [Online] https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/ [Accessed date: 30 07 2017].

3. **Laberis, B.** 20 Eye-Opening Cybercrime Statistics. [Online] http://securityintelligence.com/20-eye-opening-cybercrime-statistics/ [Accessed date: 28 7 2017].

4. **DeCovny, Sherree.** Cyber Threats: Can Financial Firms Maneuver Fast Enough? [Online] https://blogs.cfainstitute.org/investor/2017/04/10/cyber-threats-can-financial-firms-maneuver-fast-enough/ [Accessed date: 25 07 2017].

5. **Fontanella-Khan, James.** Personal data value could reach €1tn. [Online] https://www.ft.com/content/5fd7d8a8-28e5-11e2-b92c-00144feabdc0 [Accessed date: 20 7 2017].

7. **K. Soska, N. Christin.** Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In Proceedings of the 24th USENIX Security Symposium, Washington, D.C. USA, August 12-14, 2015, pp.1-17.

7. **Europol.** Massive blow to criminal Dark Web activities after globally coordinated operation. *Europol.* https://www.europol.europa.eu/newsroom/news/massive-blow-to-

criminal-dark-web-activities-after-globally-coordinated-operation. [Accessed date: 25 7 2017].

8. **Hypponen, Mikko.** Cyber Geopolitics . *You Tube.* [Online] S4x16 Events, https://www.youtube.com/watch?v=6fnGAmE1Nfw [Accessed date: 20 7 2017].

9. **PWC Research** [Online] https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/geopolitical-cyber-threats.html [Accessed date: 21 7 2017].

10. **Nurkin, Tate.** Securing the Information Domain. [Online] https://www.ihs.com/pdf/The-Information-Domain-Tate-Nurkin-Oct-2014_211035110913060132.pdf [Accessed ddate: 10 7 2017].

11. **Breene, K.** Who are the cyberwar superpowers? [Online] https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ [Accessed date: 10 7 2017].

12. Schmit, Michael N. The Law of Cyber Warfare: Quo Vadis? Stanford Law and Policy Review, 2013, 25(269), pp. 269-300.

13. **ICM Policy Paper: The Impact of New Technologies on Peace, Security, and Development**. [Online] 2016. https://www.icm2016.org/icm-policy-paper-technologies [Accessed date: 15 7 2017].

14. Pawlak, Patryk. A WIld Wild Web? Law, norms, crime and politics in cyberspace. European Union Institute for Security Studies, 2017, 23(1), p.1-4.

15. **Klimburg, Alexander**. Mobilising Cyber Power. Survival, 2011, 53(1), pp.41-60.

16. Klimburg, Alexander. Shades of Cyber Grey: Espionage and Attack in Cyberspace. [Online] http://www.fletcherforum.org/home/2016/8/15/shades-of-cyber-grey-espionage-and-attack-in-cyberspace [Accessed date: 10 7 2017].

17. Documentary. *Zero Days.* [online] Alex Gibney. DCM, 2016. https://www.youtube.com/watch?v=sYCfcnH3gno [Accesed date: 30 7 2017].