



December
2017

CYBER WORLD

Rounding up the latest in Cyber Security

In this month's edition:

Latest News

Newest Vulnerabilities

Marcelo A. O. Malagutti, Fóton Informática S.A.

Barry J. Coatesworth, SSE plc

Rafael H. Ponce, CEIS

Jeremy Blackburn, University of Alabama at Birmingham

Marco Essomba, iCyber-Security Group

A Life Less Vulnerable: The Future of Alexa & The Internet of Things

Rising Stars (Jigar Lad, EY)

Future Leaders (Edward Percarpio, University of Oxford)

Upcoming Events

 Secgate

An aerial night view of a city, likely London, with a heavy overlay of digital light trails and data streams. The image is dominated by blue and yellow light trails from traffic and buildings. In the upper right, there are red and white text overlays that appear to be "PRIMA" and "PRIMA". In the lower right, there is a blue sign that says "Aberdeen". The overall aesthetic is futuristic and high-tech.

Statecraft within Cyberspace

Marcelo A. O. Malagutti



About the Author:


Marcelo A. O. Malagutti is founder and partner at Fóton Informática S.A. in Brasil. Previously, he was Automation Manager at BRB - Banco de Brasília S.A. He holds an MA in War Studies from King's College London and is currently studying for a PhD in Military Sciences at the Brazilian Army War College in Rio de Janeiro.

The fast expansion of cyberspace brought with it a perception of freedom and spatial proximity never before experienced by the general public. With only a few clicks, almost instantly, it is possible to visit a museum in France, a library in Italy, watch a popular festival in India, buy books in the US or electronic goods in China. Users can use 'avatars' (virtual images and id's) to hide their identity, conferring on them a sense of anonymity.¹ The architecture of the Internet, perceived to offer a resilient communications alternative in case of nuclear attacks, was also considered to make communication untraceable, and thus beyond state control or censorship. All of this provoked intense debate concerning the Internet's social and national impacts. The first reflections on cyberspace, by somewhat romantic e-libertarians, suggested it would enable users to stay away from the real-world dystopia, which imprisons and oppresses everyone. It seemed to offer a quasi-utopia, the unachievable perfect world. This 'exceptionalist'² view considered cyberspace as being completely disconnected from the physical world. Real world norms would not apply there. This inapplicability of norms was also associated with the immateriality of digital assets, making digital property more ethereal. As a consequence, those who in the physical world would never steal a book, CD or BD, do consider it 'natural' to download texts, music or movies without due payment in cyberspace, in a sort of 'ideology of violation'.³ As a result, at first, the advance of cyberspace seemed to indicate that national borders would blur and the idea of state sovereignty fade.

In contrast to this exceptionalist view, there was a more conservative and isotopic one, considering the Internet and cyberspace as only a bunch of hardware and cables physically installed inside well-determined places: thus, being entirely subject to national and international laws and norms.

A third perception emerged from this debate, connected to Foucault's definition of heterotopia:⁴ places within the reality but that are still different and distant from it, such as theatres or ornamental gardens. In this view, cyberspace presents some abstract and subjective characteristics but finds itself immersed in the real world where its users live and where the devices and cables that constitute it are located. It is in the context of this heterotopia of cyberspace that the examples of its use by nation-states are framed, which suggests that it is becoming 'just' one more tool of statecraft, used for coercion. The relative anonymity, the plausible deniability, the low cost of attacks, and the 'virtual' omnipresence it provides, relatively to the kinetic world, stimulate state-sponsored actions. Cyberspace presents itself, therefore, as an object of geopolitics, in the sense of the study of spaces in international politics and the production of knowledge to subsidise statecraft and promote the power of states.⁶

In 2010, an almost unknown cybersecurity company in Belarus identified a malware, named Stuxnet, that would become the first (known) cyberweapon effectively able of physically destroy or damage hardware devices. This ingenious malware placed itself between the PLCs (Programmable Logical Controller) and its control software, generically



“ The intent of economic espionage is ‘to increase the economic prosperity or viability of business concerns in a given state’;

called ICS (Industrial Control System), of the uranium enrichment centrifuges of the Iranian nuclear plant of Natanz. These sensible electromechanical devices were then accelerated to rotation speeds approximately 40% over their regular operation speed, while the information presented to the operators in the control room indicated everything was fine. As a consequence, these devices, which are difficult and expensive to replace, were damaged much faster than expected, with nobody knowing why. This allegedly caused a delay of some years in the Iranian nuclear programme, thus supporting international efforts for coercing Iran into accepting international supervision of its programme. This malware was probably developed by the United States and Israel.^{7, 8, 9}

A different malware family, named Crash Override, and supposedly developed in Russia, has been targeting Ukrainian electrical facilities, starting with Prykarpattyaoblenergo in December 2015, and repeatedly leaving thousands with no energy during the severe Ukrainian winters. The attacks started just after the separatist war, supported by

Russia. The idea seemed to be to create difficulties for the civil population, thus reducing their support for the war effort, in a similar way as the British and the Americans used ‘strategic bombing’ against German civilian infrastructure throughout World War II. Experts estimate this malware could target electricity facilities in the United States and throughout Europe if its developers so desire, and that the diversity and age of these facilities’ cyber platforms make it almost impossible to make them resilient quickly and in the short term.¹⁰

A distinct kind of state-sponsored motivation for cyber attacks is attributed to North Korea. One set of actions targeted the SWIFT network, a Brussels-based banking consortium that runs what is considered the world’s most secure payment messaging system. The attacks, which took place in 2015 and 2016, targeted banks in the Philippines, Vietnam and Bangladesh. Even experienced security researchers declared that they never previously witnessed attacks carried out by a state with the purpose of stealing money.¹¹ These attacks seem to provide the North Korean government


```

cAnimal=setclass("Animal")

function cAnimal.methods:init(action, cutename)
    self.superaction = action
    self.supercutename = cutename
end

-----

cTiger=setclass("Tiger", cAnimal)

function cTiger.methods:init(cutename)
self:init_super("HUNT (Tiger)", "Zoo Animal
(Tiger)")
    self.action = "ROAR FOR ME!?"
    self.cutename = cutename
end

```

with an alternative way for obtaining foreign currencies, i.e. as a workaround the international economic sanctions imposed on its regime. After that, the WannaCry ransomware spread around the globe, with severe impacts on the NHS. The British government attributed the attacks to North Korea, which replied that the accusations were 'wicked'.¹²

Meddling with elections seems to be a new tool of statecraft for the Russian government. The American intelligence services accused the Russians of interfering in the US 2016 presidential elections, harming the image of Mrs Clinton and thus supporting Mr Trump, who denies all accusations.¹³ In the process, emails were stolen from the Clinton campaign and selectively leaked, and possibly altered in substance, with the apparent support of WikiLeaks. Following this incident, the French,^{14, 15} and then the Germans,¹⁶ also accused the Russians of spreading fake information in an attempt to influence the electorates in their countries. Only recently, it was British PM Theresa May's turn, when she directed the message at President Putin: 'We know what you are doing, and you will

not succeed'. These accusations were soon after supported by declarations of Mr Ciaran Martin, CEO of the National Cyber Security Centre, part of GCHQ, the British signals intelligence agency.¹⁷ The general perception is that the Russians are trying to destabilise western democracies in response to the sanctions and international resistance faced by Russia, and, more generally, in order to increase its relative power.

All of the above constitute new forms of statecraft using the cyberspace. But then there are also older, but increasingly important other uses as well: intelligence gathering, which can be used for surveillance and political or economic espionage.

The GCHQ's website notes the importance of the interception of the famous Zimmerman Telegram as one of the main reasons for the US entering World War I. It also points to the history of Bletchley Park, where Alan Turing created Colossus, the first computer in history, which helped to decipher the German Enigma code, an essential asset for winning WWII.¹⁸ These, however, were actions of passive



signal intelligence, with the interception and transcription of messages sent by others. Thus, a surveillance operation. This process on the Internet nowadays is quite similar,¹⁹ and 'the Internet is a major source of comparable intelligence power today'.²⁰

In the 'cyber' context, however, intelligence gathering is not a passive task only. The GCHQ's Code of Practice for Equipment Interference presents a list of activities that are permitted when there is 'risk for UK security', which includes accessing equipment to obtain information and 'locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information'.²¹

These activities do not need to be 'targeted' to a specific computer, device, or even user. They can be conducted on sets of equipment, for instance in an entire building or village, anywhere in the world, if there is the suspicion of a 'risk for the UK security' in that area. Its American counterpart, the NSA, has been granted the legal (by American law) right to spy on 193 countries. The exceptions are its Five Eyes partners (Australia, Canada, New Zealand and

the UK), considered 'out of limits' under the Foreign Intelligence Surveillance Act of 1978.²²

Similarly, the US Supreme Court has granted the Federal Bureau of Investigations (FBI) the right to hack computers worldwide, based on warrants given by American judges. Hence, to defend the US against espionage, the FBI is legally authorised to hack computers outside the United States. Cyber espionage targets political, military or economic information from or about another government; and includes the theft of trade secrets and intellectual property from private corporations or universities.²³

The intent of economic espionage is 'to increase the economic prosperity or viability of business concerns in a given state'; although sometimes state-directed, its 'ultimate beneficiaries may be private or semi-private entities'.²⁴ The US government frequently accuses China of 'stealing' technical, military and economic information. American authors argue in the same direction, saying that 'foreign intelligence services' engage in industrial espionage in support of private companies and that 'an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress' is stolen every year 'from networks



maintained by US businesses, universities, and government agencies', or that as national power is intimately connected with economic vitality, sustained intellectual property losses allegedly could erode US power.²⁵

But not only the US is a victim of this type of activity. The Norwegians accused the Chinese of stealing sensitive data and military secrets²⁶ and the Swiss accused the Russians of espionage against the state-owned military supplier company RUAG.²⁷ However, the facts revealed in the Snowden case in 2013 showed that the NSA is also engaged in economic espionage gaining 'enormous advantage for American industry'.^{28, 29}

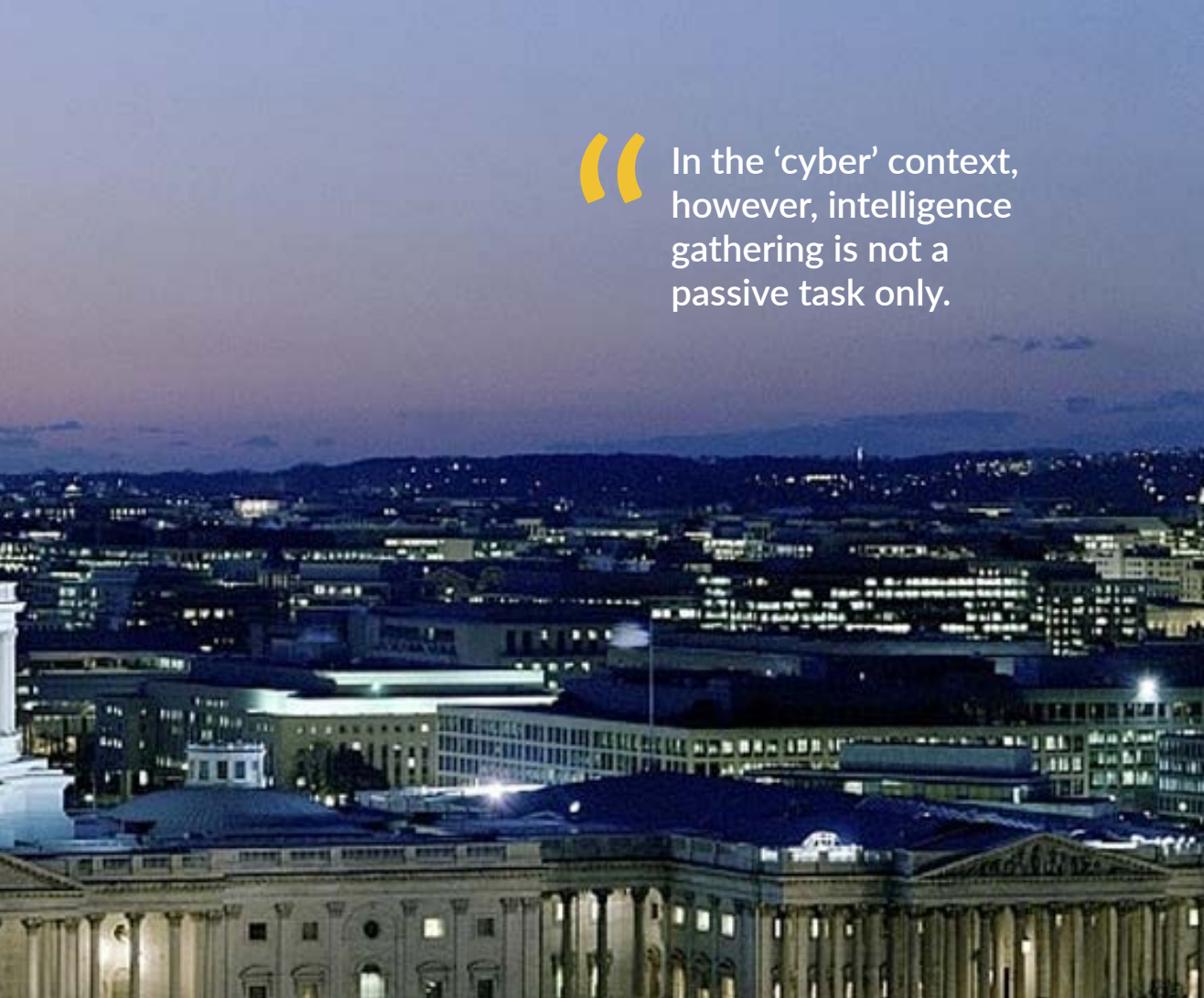
The ultimate aims of coercion and espionage are to influence decisions and to increase one's relative power. In terms of nation-states, this is called statecraft!

REFERENCES

- 1 Rid, Thomas. 2016. *Rise Of The Machines*. New York: W. W. Norton & Company.
- 2 Cohen, Julie. 2007. "Cyberspace As/And Space". *Columbia Law Review* 107 (1): 210-256.
- 3 Betz, David, and Timothy Stevens. 2011. *Cyberspace And The State: Towards A Strategy For Cyberpower*. London, U.K: Routledge for the International Institute for Strategic Studies (IISS).
- 4 Cohen, Julie. 2007. *Op cit*.
- 5 Cohen, Julie. 2007. *Op. Cit*.
- 6 Ó'Tuathail, Gearóid, and John Agnew. 1992. "Geopolitics And Discourse". *Political Geography* 11 (2): 190-204. doi:10.1016/0962-6298(92)90048-x.
- 7 Zetter, Kim. 2011. "[How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware In History](#)". *WIRED*, 2011.
- 8 Falliere, Nicolas, Liam O'Murchu, and Eric Chien. 2011. "[W32.Stuxnet Dossier](#)". Symantec.
- 9 Langner, Ralph. 2011. *Cracking Stuxnet, A 21st-Century Cyber Weapon*. TED Talks.
- 10 Greenberg, Andy. 2017. "[Crash Override: The Malware That Took Down A Power Grid](#)". *Wired*, 2017.
- 11 Perlroth, Nicole, and Michael Corkery. 2016. "[North Korea Linked To Digital Attacks On Global Banks](#)". *The New York Times*, 2016.



- 12 BBC. 2017. "North Korea Calls UK Wannacry Accusations 'Wicked'". *BBC News*, 2017.
- 13 Ackerman, Spencer, Sam Thielman, and David Smith. 2017. "US Intelligence Report: Vladimir Putin 'Ordered' Operation To Get Trump Elected". *The Guardian*, 2017.
- 14 Higgins, Andrew. 2017. "It'S France'S Turn To Worry About Election Meddling By Russia". *The New York Times*, 2017.
- 15 Stothard, Michael, and Kathrin Hille. 2017. "Macron Campaign Accuses Russia Of Using Fake News". *Financial Times*, 2017.
- 16 Reinbold, Fabian. 2017. "Germany Prepares For Possible Russian Election Meddling". *Spiegel Online*, 2017.
- 17 NCSC. 2017. "Cyber Security: Fixing The Present So We Can Worry About The Future - NCSC Site". *Ncsc.Gov.Uk*.
- 18 GCHQ. 2016. "GCHQ History". <http://www.gchq.gov.uk/history/Pages/index.aspx>.
- 19 GCHQ. 2011. "HIMR Data Mining Research Problem Book". GCHQ. .
- 20 Omand, David. 2015. "Understanding Digital Intelligence And The Norms That Might Govern It". Centre for International Governance Innovation and Chatham House.
- 21 HM Government. 2016. "Equipment Interference Code Of Practice Pursuant To Section 71 Of The Regulation Of Investigatory Powers Act 2000". London: HM Government.



“ In the ‘cyber’ context, however, intelligence gathering is not a passive task only.

22 Kedmy, Dan. 2014. "Report: NSA Authorized To Spy On 193 Countries". *Time*, 2014.

23 Cilluffo, Frank, Sharon Cardash, and George Salmoiraghi. 2012. "A Blueprint For Cyber Deterrence: Building Stability Through Strenth". *Military And Strategic Affairs* 4 (3): 3-23.

24 Cilluffo, Frank, Sharon Cardash, and George Salmoiraghi. Op cit.

25 Lynn, William. 2010. "Defending A New Domain: The Pentagon's Cyberstrategy". *Foreign Affairs* 89 (5).

26 Murdock, Jason. 2016. "Cyber-Espionage: Norway's Intelligence Chief Accuses China Of Stealing Military Secrets". *Technology*, 2016.

27 GovCERT.ch. 2016. "APT Case RUAG Technical Report". MELANI.

28 Campbell, Duncan. 1999. "Development Of Surveillance Technology And Risk Of Abuse Of Economic Information Part 2/5". Brussels: European Parliament.

29 Greenwald, Glenn. 2014. *No Place To Hide: Edward Snowden, The NSA And The Surveillance State*. United Kingdom: Hamish Hamilton.



Marcelo A. O. Malagutti
Projects Director
Fóton Informática S.A.
Brasília - Brazil