BETWEEN FICTION AND REALITY

Mircea Constantin Șcheau*

National Bank of Romania

Introduction to a Booming Universe

Topics related to cybercrime are debated with interest, which proves the impact felt by domestic users, business environment and international organisations. Even if the approach should be fairly straightforward, with reference to respecting traditional values, reality tends to contradict. The parameters that allowed us to evaluate and classify, according to the old models, a crime against the public or private domain, are modified. On the horizontal axis the time compresses, the space expands, the access points occupy distributed quadrants and the interconnected paths deepen. On the vertical axis we notice that the elements "gender and age" falls within a particularly generous range. Children or adolescents, young people, adults or those who follow the route offered by the descending slope of the Gauss bell discover their abilities that allow them to be placed on either side of the barrier that separates the good from the bad. Too few of them remain in the obscure gray area of uncertainty. All of these imply an increase in the dynamicity of the risk assessment map, allow to quickly change the shades of the penetrability degrees from green to intense red and calls in response to force the permission limit to zero.

Security companies that protect networks cto which millions of users or specialized traffic monitoring companies are connected, warn of escalating unauthorized interventions and the effects recorded as a result of malicious activities. The concept of IoT (Internet of Things) tends to become obsolete and melt together with IoP (Internet of People) in IoE (Internet of Everything). According to a report published by security company SonicWall, the number of attacks on one of the most favorite targets, IoT, has increased by over thirty-five percent in the first three quarters of the beginning of 2019, compared to the same period of 2018. It is normal somehow, because component manufacturers do not comply with the same rules and thus, major hard and soft differences occur. Regardless of the country of origin or destination, low-quality finished products, and when we say this we refer strictly to the incorporation of the protection packages, can reach the shelves alongside the top-quality ones. Without proper monitoring by the empowered organisations to check the degree of conformity, the final consumer may inadvertently interpose on the route between the producer and... the offender. I claim this because one of the current actions taken by groups that are out of the law is to check the accessibility of network nodes or terminals. Those with vulnerabilities turn into real gates for computer trojans.

* Author for contact, **Mircea Constantin Șcheau**: mirceascheau@hotmail.com
The opinions expressed in this article belong entirely to the author and do not reflect the official position of the National Bank of Romania.
Article republished from Știință și Tehnică Magazine, Year LXIX / # 93 / February 2020, ISSN 1220 6555, with the publisher's permission.

I don't think there is a loser or a winner in all this wear conflict. On the one hand, capturing a flag, approached equivalent to destroying an organized group or annihilating of a lonely hunter, is followed by the appearance of another head of the poisonous blood creature from Lena. On the other hand, the warning signals transmitted to the population during the promotion and awareness events are trying to draw attention to the potential dangers to which we are exposed. Fortunately, concerted efforts reveal out the most unusual capabilities. Enthusiasts enrolled in the gymnasium education cycle demonstrate extraordinary abilities. Maybe this is the natural result of evolution (human species). An example is a twelve-year-old girl, who was invited to DefCamp # 10, one of the biggest security conferences in Romania. Another example is one of the members of the Romanian team (see the image in figure no. 1 from the CERT-RO website), who was still in high school / college, when he was selected to join those who won in 2019 for the first time the European Champion title at the sixth European Cyber Security Challenge, competition supported by the European Union Agency for Cybersecurity and organized that year through the Romanian National Computer Security Incident Response Team, the National Association for Information Systems Security (ANSSI) and the National Cyberint Center. The outposts transferred from the virtual world to the real world are based on increasingly powerful pillars and we are witnessing the birth of a society marked by hybridization. The models are tested in the virtual world, eventually processed with the quantum computer help and later reproduced in the real world. Listed, built, or scheduled to grow from bionic cells/seeds. Paradigms inscribed in the invitation addressed to all for adapting to the challenges of the future.

Figure no. 1 Romania's team, winner of the European Cyber Security Challenge (source: CERT-RO)

States are engaged in non-aggression treaties and international cooperation, which creates the premises for strengthening the external and internal defence systems, but there are situations in which there is no need to look elsewhere for any enemy, because he is no somebody else than own ignorance or superficiality. The weakest link in a chain practically sets the maximum level up to which the chain can withstand. National and / or international communities need to focus on solutions to ensure this level is increased, and one of the directions involves providing support to the development of the security culture, regardless of domain, group, age or belonging. Romania is becoming a stronger voice and investments are not negligible at all, both in material basis and especially in human capital. Are organized national and international competitions of robotics, cyber security, innovation, between units of primary, secondary, high school, university etc. We are assisting the process of creating the trades of the future. We don't know how smart cities or the labor market will look like over a hundred years' time, but we can sense that responsibilities will change.

Some Games...Are No More Games

The universe called "Internet" provides tools and services that have been encountered until recently only in anticipation volumes. The image in figure no. 2 speaks for itself. The spectrum is similar to the human imagination and setting a limit depends on each one's power to dream. We imagine parallel worlds and build them, imagine strategies and integrate them, attract others into our dream and imagination, create alliances and conquer virtual redoubts, invent and violate rules to raise or bypass obstacles, we solve tests and jump over levels, accumulate points and sometimes we share them with those on the team etc. As in all cases encountered in real life, a price must be paid and the side effects are generated by the decision on group membership belonging - criminal or ensuring public order. Profits from cybercrime exceed USD 1.5 trillion annually (see figure no. 3) and maybe everything starts as a game until the moment ... the game is no longer game and the way back is difficult to identify. This is why efforts are being made to guide the orientation of skills starting from early ages, simultaneously with those of information and education of the older ones. In the academic environment are also active professionals from the state apparatus from several institutions, capable to present scenarios close to reality, to take on talented high school students and guide them to high profile specialized units. Actions are absolutely necessary because the new hybrid world – virtual and real – is (self) build on the go. The space is populated with drones, robots are pseudo autonomous and perform complex tasks, information transmission equipment allows high-speed data packet transfers and many other similar evolutions, whether or not they fall into a concept that I prefer to call it socio-formation.

Figure 2. Internet in a minute (source: Visual Capitalist)

Vulnerabilities do not delay to appear. Hermetization, viewed as a word in the dictionary, changes its meaning. However, we must not fall into the trap of assuming that nothing is no longer safe and anything connected to the online environment becomes automatically penetrable. However, we must adopt a prudent attitude and immediately seek the assistance of the specialists in the situation in which we feel that we have become the target on a cyberattack. Romania is among the first countries in the European Union, which has implemented with the help of the Ministry of Communications and Information Society an emergency service for cyber security, callable to the unique telephone number 1911. Natural persons, legal entities and state organisations can request support in the case of online frauds, automated (or not) attempts to break passwords, information theft, ransomware attacks, messages containing abusive content etc. It is encouraged good faith reporting of incidents, in order to be able quickly create the map of the attacks, in an attempt to identify the source and to warn the possible structures affected. There are aggressions that conceals the real intention quite well behind an avalanche that aims to block the defensive systems and there are aggressors who remotely exploit the possessor's resources, without his knowledge (e.g. cryptocurrency mining) and strive to "protect" him against other potential aggressors to keep their position active.

IoT networks, national systems of energy production and / or transport, the health system and / or the population records of a state, critical structures or substructures (etc.) are under attack and it has been proven that a malware snippet can be "successfully" remodeled and reused. Revenues may seem attractive if we approach the phenomenon lightly. Not all aggressions are motivated by immediate financial or material benefits. Conflicts in the field move to informatic (and / or biological) laboratories. Multinational companies are trying to develop products that are superior to or similar to those of their competitors and are trying

to protect their own patents. Governments that feel threatened resort to radical measures, assuming the risk of tightening international sanctions. Each conquered objective can tilt the balance or turn it into a negotiating instrument. The silent computer assassin carefully follows opponents' actions and only acts when the trigger factor is released. Until then, he is content to collect information, classify, report them and improve its own strategies.

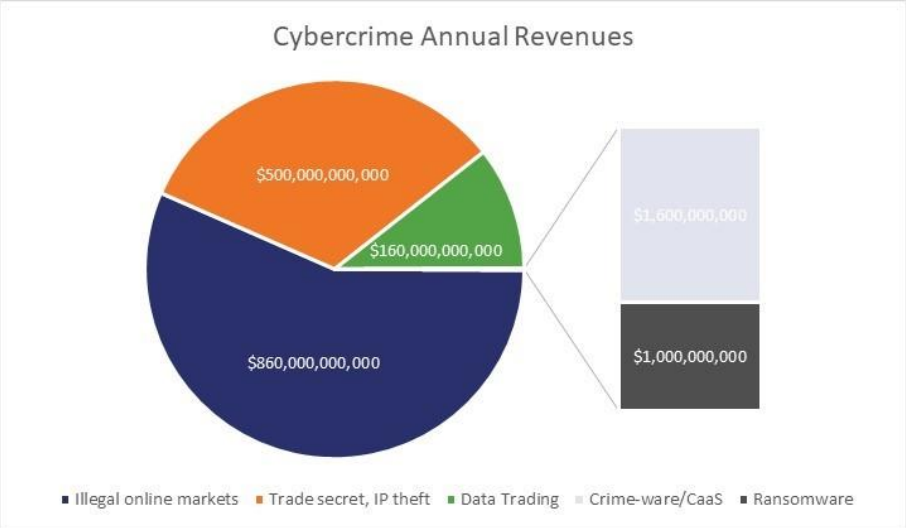

Figure 3. Incomes in a year (source: Patrick Nohe, Hashed Out, The SSL Store)

There are large-scale operations and punctual operations, regardless of whether we refer to offensive or defensive devices. They are concentrated or disparate operations, concerted or singular, with effects recorded at individual, community or global level. We can be direct victims, collateral victims, or we can take the decision to step outside the gray zone and choose to help strengthen the defence system. I don't know if it's necessary to do something extraordinary for that. I only know that it is imperative that we follow the advice of specialists to inform us, to be careful, not to treat the warnings with superficiality or to conclude, not to become the weak link of the chain. And I also know that we have a duty to help everyone around us, explain them, contribute to the dissemination of knowledge, to be actively involved or if we cannot do this, try to protect ourselves.

There are publications that have asserted themselves as message bearers, addressing all age groups and that have proven the quality of content over time. I think that deserve our support, because it is one of the channels through which the filtered / deparasited information reaches the recipients. It is also the environment where questions can be asked and answers can be received or sough. What I have said is, in fact, a plea addressed to those who want a safer world. The school as a whole has its role and society has its role but the most important in this case is its own decision. Cybercrime is part of our universe and only we can decide whether (or not) choose to be part of its universe.

Acknowledgement

The opinions expressed in this article belong entirely to the author and do not reflect the official position of the National Bank of Romania.

The original article was published in Romanian in Știință și Tehnică Magazine, Year LXIX / #93 / February 2020, ISSN 1220-6555.