THE CYBERSECURITY CHALLENGE

Cyber-threats are now becoming systemic in the world economy. Concern of all actors involved is rising, to the extent that it may lead to a global counter move against digitisation that would consequently have a huge negative economic impact. Notwithstanding progress in cloud computing and big data with, according to McKinsey, a generated annual income of between 9,600 and 21,600 billion dollars in the global economy. If the sophistication of cyber-attacks were to submerge the defensive capacity of States and organizations, we could fear more stringent regulations and policies that would in fact slow down

ParisTech Review – Are cyber-threats different for States and enterprises?

Hervé Guillou – Not really. In a cyber-world, the frontiers between public and private sector are not identified by shareholder organization or by governance. These frontiers are in fact porous, because of service activities. Private individuals need and use health services, the army needs logistics, while tax-paying companies pay their corporate taxes to the Ministry in charge of Finance. But to better understand what we are talking about, we should first define cyber-space as a rather complex combination of 3 layers running through 3 ‘worlds” making up a 9 segment ensemble.

First we have the physical layer (cables, optical fibres, submarine cables, radio and satellite links, switchgear… in short, the system that supports and transmits information.

Then comes the data processing layer with its computers, robots, server stations, protocols, directly usable software packages, like Windows, the robot control software, or software incorporated on board automobiles.

Lastly we find the information content and function layer, which is the most visible and most often associated with cyber-security: we are taking here about data, applications, information content, whether processed or stored, or cloud processed, covering activities like on line data and secure on line financial transactions (most purchase payment).

These three "horizontal" layers run through three vertical worlds that, historically, have always been separated, given that the technologies involved had their inception, standards and industrial make-up set in different worlds. These three worlds are 1° the general computer science world (IBM, Atos, Bull); 2° the industrial computer world (Catia, Siemens, Schneider) with its automats, its robotics, its 3D CAD and CAPD) tools, control protocols for digitized machines; 3° on-board computers (Honeywell, Thales) with its specialisation in real-time data processing to control aircraft flight surfaces, for example, which previously went by the name of on-board computers.

How does a cyber-threat disseminate?

Internet Protocol (IP) is vertically penetrating (because the telecomm and routing systems rendered data virtual, and simultaneously, IP is connecting general computer science with factory control and management software (for example, using SAP packages to monitor production). Onboard computers are now also coupled with industrial data processing. The "suit-case" which enables repairs to onboard data processing devices forwards the data to the vehicle manufacturer's technical centre, can download repair software patches and even order spare parts. Another example; each Airbus has 7 IPs that can be connected "at the gate" to handle catering logistics, upload the next flight schedule and once in flight send back status data. It is easy to see here that the worlds I mentioned earlier are now closely intermeshed.

What is happening today can remind us the development of international trade four centuries ago. What had been up till then coastal port-to-port trips became globalized and fabulously huge treasures began to circulate on maritime routes. This traffic brought with it boarding attacks and ship cargo capture by pirates and corsairs and, naturally, creation of military naval fleets. And viruses, occasionally lethal, began to spread.

What we are observing on Internet is exactly the same, except that the asymmetry between attackers and defenders is even more striking. For the former, it is not expensive at all to recruit 2 000 Chinese, 500 Russian or 300 Bulgarians, all of whom are excellent computer scientists. It costs far less than building a ballistic missile, a fighter jet or a nuclear reactor. Building the equipment needed for an attack and the price to “pay” for an attacker is practically zero. Moreover, they can operate almost everywhere: at half-a-dollar to hire a server station, for one million $US you can dispose of two million servers. Who has the possibility to locate the origin of an attack when two million servers, spread all round the world are involved with, say, 14 decoy countries too? Impunity is also guaranteed since very few of the institutions coming under attack opt to launch a court proceeding, given the obvious adverse effect this will have on their reputation.

We must defend ourselves, right?

Even if you want to attribute a cyber-attack, you do not have the legal means to pursue since there are practically no international laws that apply to the Internet. One of the rare international treaties in the field, the Budapest Treaty, refers to Internet in the fight against paedophilia. This is nowhere near the volumes of texts that regulate air traffic, space exploration or the seas and oceans. Victims today are in the same sort of situation as Spanish galleons in yesteryears. More and more wealth is being transported over the Net. Private persons ‘reveal’ their banking data. Design offices exchange their intellectual property. Industrialists even have their production tools on the net, with interconnected factories and suppliers connected via the e-supply chain and e-storage, their clients through e-commerce, manpower resources are managed via e-Manpower packages. Victims are static and try to make themselves known with an attractive portal web site! For the assailants the number of doors before them is growing exponentially. In year 2003, there were 500 million IP addresses in the world. In 2014, we now have 13 billion IPs and it is forecast that in 2020, the figure will no be less than 80 billion given the numbers of connected objects and industrial computerized devices and tools … Therefore nothing is easier than to attack a company via its suppliers or its external, mobile staff.

So what is a cyber-criminal seeking?

Some simply want to get rich, for example by selling ID codes of stolen credit cards. Other motivations can be sabotage or State level terrorism, or NGOs wishing to “punish” a given company, industrial espionage or theft of business data. Behind all such manoeuvres, we find not the romantic Robin Hoods but more often organized crime and what we must now refer to as an “advanced persistent threat.” For 20 euros, you can purchase a complete and valid credit card number with a withdrawal limit set by the thieves at 100 euros. If the attack has stolen some of your industrial design drawings, you must know that there is a parallel market for such intellectual property items, with which documents the follow-on purchaser can make a profit or value-add by using the contents.

How much is this war costing?

The economic wealth stolen by cyber-criminals represented 190 billion euros in 2013. The figure here only refers to direct losses. Sony Corp., for example, suffered a theft of some 1.5 million credit card ID data, worth 150 million € in direct value. But Sony then claimed 1.3 billion $US compensation from its insurance company to cover the complete shut-down of its server, infested with criminal e-trade operations, for modification of the data processing system and the public relations campaign the company had to organize to restore trust. When companies who work with the defence sector or energy utilities have there industrial drawings stolen, the economic or strategic loss can be potentially very high.

Why is it so difficult to track down the hackers?

It is already proving impossible to arrest jihadists going to Syria to fight in their ‘holy war’, as they see it, and far more impossible, so to speak, when it comes to identifying hackers … How are you supposed to track someone who is operating from a flat somewhere, with a fake IP address? Complete police units are being assembled for this very purpose, with the help of groups such as France’s Tracfin [for financial fraud mainly] and the national security services. In 2013, some 26 million malware (malevolent software) packages were identifiable, representing 70 000 new threats per day. The average level of computer “infested” round the world is about 40%.The time during which a brand new computer remains clean after its initial installation routine is 3 minutes. At or beyond that point, hackers install a little ‘botnet’ (a sleeping viral software) with the possibility therefore to wake up and run the botnet sequence at a later time, and then to use this ‘innocent’ IP to launch a cyber-attack.

How does a hacker succeed in hiding so well?

The median time to discover a sophisticated, high-level attack is calculated to be 416 days. At the French Ministry for Finance, the services preparing for a G20 summit were hacked; it took a team of 50 specialists, 4 months, working 7/7 round the clock, to eradicate the ‘cancer’. Once a hacker has penetrated your system, he/she need only wait for 24h to gain access to the daily back-up protocol and files, then for one moth to access the monthly back up, then the yearly back up, and so on. Gradually, gains access to deeper and deeper layers of your cyber-structure. When you think you have closed a door, he/she already has the keys to open all the other doors.

In short, is it impossible to effectively defend oneself?

Difficult indeed, but also an absolute necessity. It is our very survival that is at stake, simply because Internet is physically present in all our via systems: in hospital operating theatres, in our cars, in the traffic light controls, in electricity meters, in the domestic water distribution networks. Also in an immaterial way, given that the Internet serves to frame (impacting directly on) the economic resilience of a country via its banking system, for example, or again for its energy procurement policies and decisions. We can recall the case of Estonia – one of the most technologically advanced countries in the world at the time – that Russian hackers economically brought to their knees for 4 complete days in 2007.

C**an we protect ourselves at an affordable price?**

Basic computer use hygiene is primordial and can effectively counter 90% of the low-level criminal activities.70 000 lap-tops were stolen in the London Tube in 2013. 70¨of companies round the world have suffered a cyber-attack. You have to pay attention to your business. If you can erect a small ‘wall’, you can discourage many low-profile cyber-crooks who prefer easy victims. But above all other considerations, you must urgently install a master ID, based on three authentifying factors: 1° Who I am (Iris, morphology, heart beat), 2° What I possess as my ID (badge or card) and 3° What I alone know (password or secret code). If, instead of multiplying mediocre passwords that have become so numerous that you have to draw up a list, itself becoming a vulnerable item, one could access the networks using for example a biometric passport, we would be far less vulnerable. And we must now be wary of our smartphones, coming half way, as they do, between a computer and onboard data processing devices, a perfect illustration of how earlier disconnected worlds are now beginning to intermesh.

Do States and industrial majors not share a common interest to implement their own safeguard protocols and should they eventually prohibit the use of cloud computing?

Of course, the States and Majors should look after their own businesses and deploy means as necessary to protect themselves. But it must be noted that these means, duly deployed, must be homogenous throughout their system, their networks and their data handling devices and should be proportionate to the potential damage. Protection will not be the same when the risk is industrial espionage, service shut-downs or theft. As I see it, however, there is no point in prohibiting cloud technologies. We are too late here and the economic pressure is far too high to go that way. We must live with it and organize ourselves as best we can, for example by not sending just anything, any data, … to a cloud backup, protecting what w do transmit with a high-level of encryption and a professional control of one’s ID and safe transactions.

Is it possible today to guarantee absolute integrity of a corporate or institutional intranet?

No. Even if an intranet is technically and physically isolated from the rest of the world, as long as men can have access, they will constitute the weak link: lack of discipline, human factor errors, ID usurpation…

The danger is not only hackers, is it? What about possible rogue States?

States should be involved on both fronts, offensive and defensive. One of the documents revealed by Edward Snowden spelled out the fact that the NSA was spending large amounts of money and extensive resources to carry out economic espionage and even going as far as ‘infecting’ computers and routing equipment produced outside the USA from the design stage on, to ensure that the Agency retained its access privilege to all doors/portals. At the same time, the USA set up a far better regulatory and legal framework of protection to oblige families and business companies to take steps to protect themselves against cyber-attacks. Mobilising States on these issues is primordial. In France, the military forward planning law for 2014 has several articles devoted to cyber-security. Those establishments and institutions considered to be of vital interest are committed legally to submitting expert hearings. In 2013, the British Government called in the CEOs and members of the foreign trade units of all the FTSE100 companies, to issue warnings about potential attacks and solutions. Training is also important here and cyber-security modules are now generally needed in engineering and PhD courses and indeed speciality options should be opened.

And what about the corporate world?

Taking a cybernetic risk into account when framing a governance policy is essential. Generally speaking, the head of a cyber-security unit reports directly to the head of computer and data processing division, which is the worst configuration possible. Cyber-security will carry a budget allocation that is in conflict with the computer division’s overall budget, the head of which will be in a weakened position if loopholes are discovered in the system. Often too, the CIO (Computer Information

Officer) is solely in charge of general function computing and data handling, i.e., he has no links with industrial computations, or operations-intensive data processing. In short, 2/3 of the possible computerised functionalities lies outside his area of responsibility. Manpower management questions, very important for access control, also lies outside his/her responsibility. The CIO comes under the pressure of his/her hierarchy to attain scales of volume handled and to lower costs. He/she has no authority to arbitrate « cost quality trade off » between the economic value of cyber-risks and the cost of implementing adequate protection. The foreign or export division must also be totally engaged and mobilised. At one of France’s main automobile companies, it is the CTO (chief technical officer) – in charge of operations, engineering & works – who also is in charge of cyber-security. This is an excellent arrangement, because this executive has a good idea of the what onboard computer devices exist since he and his colleagues are the designers but also of general company computing since he is one of the end-users.

Are certain economic sectors better protected than others?

The most advanced companies are the banks since as far as they are concerned, general computer operations and industrial computation operations are the same. Certain other sectors, in contra distinction, are more lax. Certain turn-key factories are commissioned without any cyber-security measures. We once showed an oil refinery operator in the Middle East – the largest of its kind in the world – that the whole plant could be brought to a halt remotely in less than 10 hours. One only needed to pirate the IP of a control panel, then modify what was displayed on the operations screens and induce the technicians to take ‘corrective’ measures that in this configuration would lead to plant accidents. You have to know how and when to invest appropriately. When the mobile team of an oil Major learns that all their exploration maps and files have been stolen, they have, in essence, lost some very valuable arguments when it comes to negotiating commercial rights and their employer-company will surely regret not to have purchased a few encryption-fitted mobile phones.

And the best line of defence is… ?

The main factor is real-time reactivity. To reduce the level of damage, you must firstly shorten the time after discovery of an attack. Probes should be installed in the system environment. High-level cyber-criminals will still get through, while others while leave faint signal of their stay. A desk position that remains "active" during non-work hours, a data stream transmission using a usual protocol. When there is a suspicion, we can go look for the intrusion and identify. Second key point here is to be selective inasmuch as you cannot protect everything all the time. The data handling systems should be segmented into non-miscible units, i.e., threat-proof, with professionally managed system access authorizations.

How do you build up a strong cyber-security offer?

What is called high-grade security is very confidential and represents an economically narrow slot. An example, the military communication codes used in nuclear sites. The general public market here is totally in the hands of the Americans. They have bought out all the competition and built several billion dollar groups 'verticalized' round Intel, Microsoft or Cisco. For mid-grade security measures, viz., assuring the defence of large, vital industrial groups, there are not really any offers in Europe given that the subject matter was largely ignored. More than 95% of those companies that propose solutions have capital assets amounting to less than 5 Meuros. Most often, it is the start-ups that are undercapitalized, offering a limited range of products, fragile R&D activities and who have a hard time trying to expand their business, especially in foreign market-places. Large industrial groups hesitate to outsource their cyber-security for fear of running into problems associated with re-deployment and renewed staff … In the USA, the Department of Homeland Security, who hold joint control over the

National Security Agency (NSA) have a total turnover of 50 billion $US and invest 3 billion $US each year in cyber-security with 80 000 persons on the associate industrial payrolls. Here we can see that we have a sector that demands consolidation. In France, what is called « Plan 33 » a pact for cyber defence in a renewed industrial France, written into the framework of a the recent creation of a specifically French sector for security measures is both a step in the right direction and excellent news.

The French CNIL (national commission for computer uses and liberties) and foreign counterparts focus on protecting individuals. Should similar institutions be set up to protect the corporate business world?

CNIL, inasmuch as its remit is to protect private persons against potentially abusive use of the personal data, is still interested in the same persons when they are at work. The Commission therefore has a high-profile presence. But the CNIL is not in charge of protecting merchant goods or corporate data. That is the company's responsibility, with possible support and advice from France's ANSSI (national agency for information system security) or from trustworthy cyber-security companies that we can see developing today. The only real problem here is that today these companies are too small. The cyber-security sector of activities should be organized and rapidly consolidated.

Source : http://www.paristechreview.com/2014/04/25/cybersecurity-challenge/