LUC-FRANÇOIS SALVADOR

CEO of Sogeti

Your Excellencies, Ministers,

Distinguished Guests,

Ladies and Gentlemen,

Our modern world is interconnected more than ever. Sending an email, making a bank transfer, ordering online or booking your flight directly on your mobile has never been as easy and fast as today.

- About 50 billion devices will be connected to the Internet in 2020, most of them barely protected, which implies as much potential doors for hackers to intrude in our machineries, our companies, our home and personal lives.

IT and technology are at the **heart** of our civilizations and organizations.

- The increase of **networking** and connections enable our organizations to become more efficient, more productive and better informed.

- **Data and Information Access** are key assets for every individual, every company and every state. Thus, IT and technology have become vital for **decision making**.

- This allows **processes optimization and industrialization** such as railway tracks switching operability, air traffic control, gas and electricity distribution or chlorine water supply.

However the **ever-increasing use of technology goes with the lack of understanding the consequential stakes**, especially amongst the young generations. *"We don't care how it works, as long as it works".*

We become an easy target and vulnerable. All our strong points turn out to be our weaknesses.

As first, **hacking** was considered as a **game**, a playful hobby for a small group of people. Then it became a **political or ideological tool** such as the *Anonymous*, impacting the public opinion and manipulating the crowds – as we saw it during the *Arab Springs*. But as powerful as they are, they are still in a non-detrimental mindset. Of course we can argue that they are "*haktivists*" organizing **civil disobedience** protestation more than direct or radical actions. But when it comes about publishing confidential information, they could make some serious damages including human lives (cf. US diplomatic cables leaks published on *Wikileaks* that put in danger US governmental agents, known as ***Cablegate*** in 2010-11). What is more disturbing is the criminal use of networks and technologies which happen a million times every day. **Cyberspying** is also becoming usual. Yet non existing about **cyber terrorism** is only a matter of time before it happens.

The **borders between all of these actions are fuzzy** mostly due to the topology of cyberspace. Despite the regulation that rules the web, a **grey area** still remains where well organized people can operate with impunity. Hackers and cyberspies understood it well. The cyberspace provides the perfect cover making them very hard to detect. The complexity of cyber attacks makes them even more confusing. No flags. No uniforms. Your friends dress like your enemies and your enemies dress like your friends.

So what make cyber attacks so difficult to prevent?

- First of all, there is **no smoking gun or warnings**. Indeed hackers benefit from the surprise effect amplifying the fears of the unknown.

- There is also a **time uncertainty** especially in spying operations. A Trojan or a worm could remain dormant in an IT system for months before being detected and measuring the amount of information stolen from your system. Each night, thousand gigabits of technological and strategic data are stolen from thousand of computers of our Western companies.

- Moreover it is **discreet**, as the nuclear weapon secrets at its time, the knowledge of building a cyber weapon still remains in hands of few individuals. For most people, the lack of understanding in their devices is sadly another key for successful attack. Yet a cyber attack can cause **significant damages at a very large scale**, **for long period of time and at low costs**. Nowadays it is easier and cheaper to order online a cyber attack targeted to an individual than buying a gun. Under cost cutting plans and Defense budget reduction pressures, cyber warfare become an economically interesting and credible option for any harmful-minded organizations.

- Finally, most of the time a cyber attack is not claimed. Identifying the author remains highly complex and depends on few characteristics like concordant items of evidence, the language used, the names of commands and so forth.

The most harmful identified ones happened in the Middle East.

It started with **Stuxnet** in June 2010. Stuxnet is believed to be the first malware to hit on specific critical infrastructure systems. It was designed to break down centrifuges at Iran's Natanz uranium enrichment plants. The sophisticated virus spreads via USB drives and installed through several unknown Windows breaches called Zero Day vulnerabilities. Using stolen digital certificates, Stuxnet was aimed at Supervisory Control and Data Acquisition systems (SCADA) that controlled industrial processes, while infecting Programmable Logic Controllers (PLC).

Some others worms have been discovered in late 2011 such as **Duqu** and **Gauss** mostly designed for spying operations: stealing data, installing backdoors, capturing passwords. More insidious malwares, **Mahdi** and **Flame,** discovered in early 2012, were built for the same spying purpose.

The latest known cyber attack was **Shamoon** targeting to the Saudi Oil Major Aramco. It all started by a propaganda on social networks (Facebook, Twitter) few days before the attack. August, 15 Aramco said to be under large scale cyber attack and overnight, completely crashed a total of 30,000 computers hard disk drives. Experts say that this sabotage operation was much easier to undertake than the Stuxnet one, because the malware did not have to stay undetected for long. So it can happen to any organization, at any moment, without warning. Shamoon was scheduled to hit at a specific time and relayed by a strong propaganda. Later on, a massive **DDoS** attack stroked at top 20 US banks websites putting down their servers due to millions of requests, emails and spams at the same time (Distributed Denial of Service).

Now let's imagine an attack on refineries in a large harbor city. All the navigational instruments blocked. All communications towards firemen and emergency services shut down. At the same time, the banking networks hacked. Hackers create panic and chaos.

Lately, a scientist[1] proved that even radio controlled Pacemakers can be easily hacked by a virus causing the sudden death of its bearer by electrical shock. Worse, these viruses can spread out to other bearers and kill them too. This is no longer science fiction, it exists today.

[1] Barnaby Jack from IO Active at the 2012 Breakpoint Security Conference.

It raises the following question:

Are the States ready to take on such threats?

Fortunately some responses already exist.

Some in **Cybersecurity reinforcement**:

- Such as the NATO initiative Tallinn based of Cooperative Cyber Defense Centre of Excellence established in the wake of 2007 the attacks on Estonia and the Bronze Night events. It is a research center, mostly in legal field but no operational oriented. There are currently 11 countries[2] involved within the centre and France will join them soon.
- Besides France also develop its own national agency for information systems security: ANSSI since July 2011.

Other responses are **combat oriented by purchasing cyber capacities.**

- In 2010, the USA have developed the US Cyber Command to centralized command of cyberspace operations, organized existing cyber resources and synchronizes defense of US military networks.
- Israel created the Strategical Cyber Bureau which works closely with the "Unit 8200" Negev desert based to work on cybersecurity of critical infrastructure, to counter cyber-terrorism, to identify vulnerabilities in the critical systems including digital networks used in banking, energy plants and other civilian infrastructure.

These examples show the good will and the rise of a new cultural change in the usual military mindset.

Nonetheless, it raises another question:

Is there any strategic doxa?

Answer is not so clear. Of course, there are some sketches of thoughts from think-tanks or from the US Cyber Command such as *Manual for Cyber Warfare*[3] or the NATO *Tallin Manual*[4]. But there is no real doctrinal actions planning in the long run – at least visible.

It will be wise not fall into the trap of short memory. Each attack brings its own wave of strategies, policies and statements. Since Shamoon, Estonia 2007 event is almost forgotten in public opinion. We need to be very cautious and vigilant because a cyber attack could be as sudden, shocking and stressful as it could be discrete, durable and unknown.

The main issue of cyber warfare is the **Breach of Trust** in our IT systems. Not even speaking about a breach of operability on SCADAs which would be the worst scenario. Simply the hacking of a bank or the social security website

[2] Estonia, Germany, Italy, Latvia, Lithuania, Poland, Slovakia, Spain, Hungary, USA, Netherlands.

[3] Field Manual (FM) 3-36 provides US Army doctrine for electronic warfare (EW) planning, preparation, execution, and assessment in support of unified land operations. The principle audience for FM 3-36 is Army commanders and staffs at all echelons. This FM serves as an authoritative reference for personnel who: Develop doctrine (fundamental principles and tactics, techniques, and procedures), materiel, and force structure. Develop institutional and unit training. Develop standard operating procedures for unit operations. Plan, prepare, execute, and assess EW.

[4] Published in November 2012 and written at the invitation of the Centre by an independent "International Group of Expert", is the result of three years effort to examine how extant international law norms apply to this new form of warfare. The Tallinn Manual pays particular attention to the *jus ad bellum*, the international law governing the resort to forces by states as an instrument of their national policy, and *jus in bello*, the international law regulating the conduct of armed conflict

would cause the breach of trust from consumers, users, or citizens throughout our modern societies. State authority would be at stake under the pressure of citizens' mistrust and dissatisfaction. Taking into account our ever-increasing use of technology, not to say technology dependence in every aspect of our economic and social environment, our world is a lot simpler to put an end than what we think. We are potentially dealing here with a global breach of trust that requires constant diligence and awareness in order to be prevented.

Thank you.