УДК 004.056.53

GILLES RAYMOND,
AMANTUR RYSPAEV,
GULNURA KYDYRALIEVA
France, Britanny, The University of Western Britanny
Kyrgyz National University named after Zhusup Balasagyn, Bishkek

THE CYBER PROTECTION AT THE MINISTRY OF DEFENSE IN FRANCE

Киберзащита в Министерстве обороны Франции

I. Presentation
II. The different types of threats and attacks
III. The ten commands of Cyber Security
IV. Conclusion

Annotation

Annotation: *This article provides an overview the cyber security at the Ministry of the Armed Forces in France. Nowadays the cyber protection has very important role in the information and communication systems. When it concerns to the sensible branch as the Ministry of the Defense every user is a key player in the Cyber Security. The article does not claim to be exhaustive, but aims to provide a good tarting point for related research.*

Аннотация: *В статье дается обзор кибербезопасности в Министерстве обороны Франции. В настоящее время киберзащита играет очень важную роль в информационных и коммуникационных системах. Когда речь идет о разумной отрасли как министерстве обороны, каждый пользователь является ключевым игроком в кибербезопасности. Статья не претендует на то, чтобы быть исчерпывающей, но имеет целью обеспечить хорошую отправную точку для соответствующих исследований.*

Keywords: *protection, information system, cyber defence, french defence and security policies, cybersecurity, organisation of national security and defence; cyber terrorism; cyber war.*

Ключевое слово: *защита, информационные системы, киберзащиты, французская политика обороны и безопасности, кибербезопасность, организация национальной безопасности и обороны, кибертерроризм, кибервойна.*

Introduction

We live in an information society and in a “cyber” era, premised on the widespread use of connected information technologies and telecommunications, most notably the Internet.

It is the set of computer processes aimed at protecting the data transiting on an Information System. This is the desired state of resilience to cyberspace events that may compromise the availability, integrity, or confidentiality of stored, processed, or transmitted data, and related services, such as information and communication systems. (CIS) offer, or make it accessible.

Three dimensions condition cyber security:

1. A cyber security primarily uses CIS protection techniques for computer risk analysis to design and prepare less vulnerable information and communication systems. These elements are grouped under the term cyber protection.
2. It also relies on the implementation of a computer fight defensive which constitutes the repressive component. This component belongs to the cyber defense and gathers the technical and non-technical measures allowing a State to defend its information and communication systems.
3. Finally, cyber security is based on a mastery of information systems that must be administered, operated and maintained by teams of operators dedicated to the continuity of CIS. This notion is called cyber-resilience.

Why CYBER awareness at the Ministry of the Armed Forces?

- It is obligatory

- Any information is sensitive

- Direct or indirect threats, internal or external
- Obligations, rights and duties of each
- Basic rules of computer hygiene

These points ensure the confidentiality, integrity, availability and non-repudiation of the data.

I.Presentation

□ All Defense workers are personally and legally RESPONSIBLE

□ Everyone must sign a Certificate of Recognition of Liability
(ARR) It is necessary to read it carefully.

The Cyber Protection.

Every Defense user is a key player in the Cyber Security.

This is not just a matter of specialists, it concerns all of us.A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences[1].

II. Different types of threats and attacks Accidental or unintentional threats • Natural (Tornadoes, earthquake ...)

- Material (age, heat ...)
- Human

Intentional or deliberate threats

- Greedy
- Playful
- Strategic
- Terrorist
- Ideological

Cyber Attacks

CYBER CRIMINALITY:

The term "cyber crime" covers all illegal activities on the internet. The most common cases involve fraud, counterfeiting and unauthorized access to third-party data. But the threat is still underestimated by users. The official portal for the reporting of illicit content on the internet is recording a decreasing number in the field of cyber crime. If the losses were still 416 million euros in 2015, this figure climbed to 399 million euros in 2016. In addition, there are a large number of unreported cases that can not be registered by the authorities.

CYBERTERRORISM

Deliberate and large-scale disruption of computer networks, particularly personal computers connected to the Internet, using viruses, etc.

Cyberattacks can overlap with cyberterrorism, but there are several key differences. Cyberterrorism is not necessarily a response to an action, but rather planned and orchestrated due to a particular political motivation. Similar to terrorism, the goal of cyberterrorism is to gain attention and cause mass panic and fear amongst civilian populations; while terrorists use bombs, cyberterrorists use the internet[8].

CYBERSPLANTING

Spying on the Internet.

THE CYBERGUERRE

Electronic attacks against computer systems are used as a means of propaganda and disinformation, or to paralyze the vital activities of a country.

Threats & Attacks OMNIPRESENT

- Imperative respect of the rules of behaviour

III. The 10 Commandments

1. Move the removable media through the white station or data insertion point (PID) of the networkin question, and do not connect any personal media to a work computer.
2. Delete all unnecessary data from your USB keys. The USB key is not a storage tool.
3. Inform immediately any abnormal behaviour of your CYBER correspondent who will contact therelevant organizations and guide you in the actions to be taken.

Procedure to be applied in case of viral attack

- DO NOT USE the keyboard and the mouse
- DO NOT DISCONNECT the network station and ESPECIALLY DO NOT DISCONNECT IT
- Gather all used computer media
- Warn all users of the computer and computer media
- PREVENT your "Cyber servant"

4. Surf cautiously at the Internet

There are several potential risks associated with browsing and publishing personal data on the internet:

- Pirate websites imitating official websites
- Defaced websites
- Social networks (Facebook, Twitter, Youtube ...)

5. Use passwords that are truly robust and secret, do not let them be accessible
6. Lock your work session when you temporarily leave your workstation.
7. Communicate only your professional email address to people you trust.
8. Be careful with the emails you receive.

Check the sender, carefully click on the links and open the attachments carefully.

9. Adapt the transmission means according to the sensitivity of the information.
10. Do not try to circumvent the security policy.

Organising for Cybersecurity and Defence

The National Information Systems Security Agency (ANSSI) France has organised its cybersecurity and defence in a centralised manner in line with its historic state traditions, quite unlike the approaches undertaken by the United States and Germany for example [5].

As noted, ANSSI is the highest standing cybersecurity and defence agency in France [4]. Reflecting the importance of cybersecurity in the eyes of the French state, ANSSI is under the direc4t authority of the Prime Minister. More precisely, ANSSI is part of the General Secretariat for National Defence and Security (Le Secrétariat général de la défense et de la sécurité nationale, SGDSN), which assists the Prime Minister in the exercise of his defence and security responsibilities and works closely with the Presidency of the Republic. ANSSI's current Director General is Guillaume Poupard [7].

Created in 2009, ANSSI succeeded the Central Information Systems Security Directorate (20012009) and the Central Cipher and Telecommunications Security Department (1986-2001). In 2010, ANSSI acquired the role of provider of cyber defence, in addition to the cybersecurity role mandated from its inception. The agency's budget for 2014 amounted to EUR 80 mln, of which 30 mln were spent on salaries. At the end of 2014, the agency had over 420 employees, with the target of 500 employees by the end of

2015. ANSSI's mission is four-fold: to detect and implement early reactions to cyber attacks; support the development of trusted products and services for state institutions and economic actors; advise and support state institutions and operators of vital infrastructure; as well as raise awareness and actively communicate on cyber threats.

The agency itself is divided into four sub-directorates

- The Information Systems Security Operational Centre (Le Centre opérationnel de la sécurité des systèmes d'information, COSSI) is responsible for threat analysis; identification of vulnerabilities; and responding to ongoing cyber attacks by characterising the attack, designing countermeasures, and helping to resolve them. COSSI hosts the CERT-FR—the French Computer Security Incident Response Team (CSIRT)—and the Centre for Cyber Defence, which works closely with the Analysis Centre for Defensive Cyber Operations in the Ministry of Defence (Le Centre d'analyse de lutte informatique défensive, CALID).

- The Expertise Sub-Directorate (La Sous-direction Expertise, SDE) is responsible for maintaining ANSSI's science and technology expertise and applies it in-house and with its customers.

- The Secure Information Systems Sub-Directorate (La Sous-direction Systèmes d'information sécurisés, SIS) conceives, proposes, and delivers secure information systems for state institutions and operators of vital importance.
- The External Relations and Coordination Sub-Directorate (La Sous-direction Relations extérieures et coordination, RELEC) co-ordinates ANSSI's relations with state institutions, the business sector, international partners, as well as the public. Moreover, ANSSI can employ the Government □ Transmissions Centre, which assures the security of government communications.

CONCLUSION

Cyber protection is a crucial element of ics (Information and Communication Systems)

Everyone is the main player, security is everyone's business. It only takes one infected post to cause the destruction of thousands more.

Any incident related to an intentional breach of the security policy is likely to result in disciplinary and criminal penalties.

While France has come a long way in terms of its cyber policies, organisation, and budget, the continuing rise in attempted and successful cyber attacks means that these efforts have been only a start [6]. Much more needs to be done across the public and private sectors. The budget allocated to counter the cyber threat will play a big role. In times of austerity, holding the line or ever increasing budgets for security and defence is difficult – to say the least. However, France has realised that its national sovereignty would be undermined irreparably if it does not allocate the necessary financial resources [2]. One positive sign in this regard is the adoption of a modified LPM for the years 2015 to 2019, which was passed in April 2015. The modified LPM continues the strong focus on cybersecurity and defence, most importantly promising an additional EUR 1 bln on cyber defence and the creation of 500 new jobs in cyber defence. In short, the current level of the cyber threat, the political commitments across party lines, and the necessary money behind the cybersecurity and defence drive all bode well for French cyber efforts. The next big step will be the adoption of the new national cyber strategy, which the Prime Minister plans to publish in the summer of 2015.

References 1. Bernard Cazeneuve, at 7 th International Cybersecurity Forum, Lille, 20 January 2015, "FIC2015 Discours de Bernard Cazeneuve et Thomas De Meziere," International Forum on Cybersecurity, accessed on 16 July 2015, video available at https://www.youtube.com/ watch?v=v9NPGaVHqmU.

2. President of the French Republic, The French White Paper on Defence and National Security, 2008, accessed on 16 July 2015, available at http://www.ambafranceca.org/IMG/pdf /Livre_blanc_Press_kit_english_version.pdf.

3. Prime Minister of the French Republic, Information Systems Defence and Security: France's Strategy, 2011, accessed on 16 July 2015, available at http://www.ssi.gouv.fr/uploads /IMG/pdf/2011-02-15_Information_system_defence_and_ security__France_s_strategy.pdf.

4. President of the French Republic, The French White Paper: Defence and National Security, 2013, accessed on 16 July 2015, available at http://www.rpfrance-otan.org/IMG/pdf/ White_paper_on_defense_2013.pdf?572/67a412fbf01faadf4bbac1e9126d2e32f03f0bc0.

5. See "Communiqués de Presse," ANSSI, accessed on 16 July 2015, available on http://www.ssi.gouv.fr/presse/communiques-de-presse/.

6. Government of the French Republic, "La nouvelle France industrielle: Présentation des feuilles de route des 34 plans de la nouvelle France industrielle," accessed on 16 July 2015, http://www.economie.gouv.fr/files/files/PDF/nouvelle-franceindustrielle-sept-2014.pdf.

7. Ministry of Defence of the French Republic, "Pacte Défense Cyber: 50 mesures pour changer d'échelle," 2014, accessed on 16 July 2015, available at www.defense.gouv.fr/ content/download/237702/2704402/file/Pacte%20D%C3%A9fense%20Cyber1.pdf.

8. Bernard Cazeneuve, at 7 th International Cybersecurity Forum