Securing the Cyber Space in the Light of State Sponsored Activities

MAY 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2017
Reproduction is authorised provided the source is acknowledged.

Securing the Cyber Space in the Light of State Sponsored Activities

Motivation. In a society that moves ever faster digital, cyber security is crucial. Today, many critical infrastructures and commodities depend on the correct functioning of communication services. But, that is only the beginning; with the aid of computing as service, big data and artificial intelligence based applications are ready to hit the mass market. This will increase the dependency on information and communication services even more. Unfortunately, this development creates also opportunity for less well-meaning subjects. Already today criminal business models, terrorist activities, and state sponsored attacks on cyber infrastructure are on the rise and there is no indication that this trend will turn around soon.

Quite some time has passed since details about ongoing malicious state sponsored activities in the cyber space have been publicly revealed.[1] Since then, state sponsored activities ranked as one of the top concerns for most governments and executives worldwide and EU.[2] This development is a consequence of various revelations[3] and high-impact cyber-security incidents that are allegedly attributed to cyber-espionage campaigns[4,5,6,7].

Fuelled by the frequent headlines on state sponsored surveillance, a debate is taking place concerning cyber security, data protection, and privacy[8,9,10]. It is a necessary debate to reinforce trust in and resilience of IT infrastructures and services, and the efficiency of their protection measures. Moreover, such headlines serve as trigger to understand and assess the bigger picture of variants of state sponsored activities that might include: cyber-espionage, non-lawful state surveillance, cyber-sabotage, and cyber-war. The interplay of actors, motives, capabilities and tools involved in these aggression acts need to be analysed and understood, prior to the development of proper cyber-defence strategies.

Before getting into ENISA's activities to secure the EU's information networks, we need to reflect on the term *hostile state sponsored cyber activity*. Throughout this paper, we consider that any state sponsored activity that undermines the information and network security of another state or its of its citizens as such an activity. Note, in the past it was often stated, that the quality difference between state sponsored and criminal activities was mainly a difference of resources. With computing resources as a services and the

[1] http://security.blogs.cnn.com/2013/06/25/terrorists-try-changes-after-snowden-leaks-official-says/, accessed April 2017.

[2] https://euobserver.com/foreign/136503?utm_content=44319878&utm_medium=social&utm_source=twitter, accessed April 2017.

[3] https://wikileaks.org/ciav7p1/, accessed April 2017.

[4] http://www.reuters.com/article/us-usa-russia-cyber-idUSKBN14S0O6, accessed April 2017.

[5] http://www.telegraph.co.uk/news/2017/03/19/german-cybersecurity-watchdog-raises-attack-alert-level/, accessed April 2017.

[6] http://www.telegraph.co.uk/news/2017/03/15/pro-erdogan-hackers-hijack-twitter-accounts-hurl-insults-netherlands/, accessed April 2017.

[7] http://justitie.eenvandaag.nl/blogs/71907/hundreds_of_cyber_attacks_by_russia_and_china, accessed April 2017.

[8] https://sipa.columbia.edu/news-center/article/experts-discuss-cyber-espionage-propaganda-and-russia, accessed April 2017.

[9] http://www.motherjones.com/politics/2017/02/what-russia-european-elections, accessed April 2017.

[10] https://epthinktank.eu/2017/02/03/cyber-security-what-think-tanks-are-thinking/, accessed April 2017.

existence of botnets, this distinction is not valid anymore. As a consequence, a system that is vulnerable to state sponsored attacks, is most likely as vulnerable to criminal activities.

As network and information security (NIS) and hostile state sponsored activities have opposing objectives, these developments have consequences for cyber security: many voices refer to the failure in protecting data in cyber space; while others, e.g. security experts, see it as proof of a long known, yet unspoken threat, the so-called "elephant in the room". Regardless of the view taken, it is a fact that the cyber security community needs to digest these developments, reassess their purpose, scope and develop efficient defence strategies. All this is of paramount importance to the European Union and Member States and is being followed closely by EU bodies and ENISA in particular.

ENISA policy context. In the light of what is at stake, ENISA is mandated to "[…] assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet […] requirements of network and information security […] thus contributing to the proper functioning of the internal market"[11]. In this context, ENISA is setting out its position with regard to recent discussions concerning the interplay and balance between cyber security and data protection. Moreover, ENISA considers its involvement in these discussions to be a natural consequence of the fact that this debate concerns potentially "[…] unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems"[12].

ENISA's related activities. While examining cyber-security topics in the context of security, resilience and privacy, ENISA has touched upon numerous aspects and topics that are related to cyber-defence against state sponsored aggressions. Yet not completely covering all aspects of this cyber-threat, this work is a good basis for i) elaborating on available protection measures and assess the level of mitigation of this threat and ii) understanding gaps and additional topics to be addressed in the development of corresponding defences.

Here we need to point to ENISA's work on the assessment of cyber-security trends of current cyber-threats. This work covers developments regarding state-of-play of state sponsored activities and rates their importance. A further group of related ENISA material covers technologies to defend infrastructures. Worth mentioning in this context is the work on cloud computing, big data, encryption, and privacy enhancing technologies, as well as incident sharing, notification and coordination schemes. In the reminder of this paper, we summarize relevant findings in those areas. Aim of this discussion is to underline the relevance of this material in reducing the attack surface of technological systems to any attack including state sponsored attacks.

Trends in cyber security threats. ENISA has assessed the major developments regarding the cyber-espionage threat.[13] The assessment covers related threats, risks, and their impact, which follow recent state sponsored activities based on information published in the media. With focus on state sponsored activities, we assess the following trends in the domain of cyber security:

- US agencies maintain many cyber-tools – also referred to as cyber-weapons – to hack their opponents.[3]

[11] REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 21st May 2013, Art. 1, 1.
[12] REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 21st May 2013, Art. 1.3
[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, accessed April 2017.

- Cyber-operations have been launched to affect important political events in other countries, e.g. in the form of influencing public opinion during elections; such attempts are seen as most serious influences of democracies.
- Governments are increasingly targeted by cyber-espionage campaigns.
- State sponsored activities occupy very skilled and capable actors, posing thus a great challenge to the defenders.
- When called upon to defend their infrastructures, countries will need to set up novel structures and capabilities, such as cyber-police and cyber-army. Such developments lead to impressive campaigns that happen as we speak.[14]
- Current legal frameworks may be insufficient for ruling involvement of democratic states in cyber-warfare activities. Member states will need to re-consider their laws to accommodate courses of defensive actions[15].
- Due to increased interest in cyber-defence/cyber-attack capabilities, there will be a race in staffing required positions. This trend may lead to blurry lines across lawful and malicious actor engagement.[16] This is a serious risk.
- A plethora of novel attack and defence scenarios will be launched/developed when all these new players come to unfold their activities in the cyber-space.
- Vendors of services will face challenges when called upon to fulfil security requirements related to state sponsored activities, such as maintenance of data confidentiality, data quality, and data integrity.[17,18]
- Key industrial players – notably the ones acting in the supply chain of critical infrastructures – will need to coordinate their security activities (i.e. policies, architectures, response, continuity) to be in the position to withstand state-sponsored attacks.

Through prospective ENISA work, these trends will be continuously validated and also considered when applicable. Examples are the ENISA activities following up on threats emerging from these threat actors; ENISA activities leading to the protection of critical infrastructures, coordination of European response team, ENISA following relevant policy and technological developments, observing market reactions and liaising with industry, identifying proper protection requirements, supporting relevant stakeholders.

Apart from these trends, the concerns of industry and consumers need to be taken into account. These concerns are related to the trust of existing digital services and products and might affect the relevant market segments. Given the importance of the Digital Single Market to the EU's economy and society, its protection from cyber threats is crucial. This, in turn, demands an effective European industry to supply the necessary NIS products and services.

Technologies to defend Infrastructures. The above listed threats should make clear that we need use any tool at hand to protect our information society. Cryptographic tools are one of the most important weapons against cyber-attacks. These tools provide confidentiality and integrity to electronic

[14] https://www.bundeswehrkarriere.de/it?pk_campaign=Digitale%20Kraefte%20Cyber%20Kick-Off&pk_kwd=SPON_SB_X00118159 , accessed April 2017.

[15] http://www.spiegel.de/politik/deutschland/bundeswehr-wie-weit-duerfen-die-hacker-der-regierung-gehen-a-1141966.html, accessed April 2017.

[16] http://www.zdnet.com/article/whats-the-difference-between-state-backed-hackers-and-cybercrime-gangs-nothing-at-all/, accessed April 2017.

[17] https://www.good.is/articles/facebook-trust-news, accessed April 2017.

[18] https://www.bloomberg.com/politics/articles/2017-04-05/merkel-cabinet-backs-facebook-fines-to-stem-fake-news-in-germany, accessed April 2017.

communication services and data stores. However, there has always been a tension between security, in the sense of public safety and law enforcement, and the use of cryptographic tools. This tension has resurfaced in the light of recent terrorist attacks in Europe.

Law enforcement agencies report an increasing number of cases where electronic evidence cannot be interpreted due to encryption. In this light some politicians ask for quick solutions from the IT industry that provide access to encrypted information, which reopened a debate on key escrow and backdoors. Throughout this debate, advocates of cryptography have often been discredited by the motion that "if you do nothing wrong then you have nothing to hide" and strong confidentiality is often presented as threat to security.

However, this argument falls too short, backdoors and key escrow even when implemented with the best intentions, is a weapon that can be easily turned to its owner. The implementation of such means will make systems more complex and it will introduce new vulnerabilities which might be used by criminals, terrorists and unfriendly state actors, as detailed out in ENISA's position on lawful interception.[19]

Another technology area that comprises an interesting target for state sponsored activities is big data. It will allow for obtaining massive information about a big sample of intelligence sources. Big data analytics and hyper computing are the prospective tools for data collection, data mining and trend analytics; the computing power these mechanisms can provide will minimise the time of analysis and at the same time maximising the granularity of the result. This can be achieved due to the large volume of information included. Increasing the volume of data, increases the attack impact[20] by providing massive information. Based on recent ENISA reports[21], eavesdropping, interception and hijacking (cyber espionage indications) are threats of high probability in Big Data, as the software distributions rarely have protocols that ensure data confidentiality and integrity between communicating applications enabled or configured properly (security by default techniques, removing back doors). Moreover, as this model is based on the Cloud computing business model, Big Data also inherit the challenges Cloud presents.

Finally, as regards Cloud Computing, ENISA has pointed out the risks related to foreign states' national interests and the interception of data transfers over the Internet in its Cloud Risk Assessment[22]. When it comes to the threat of data being accessed with the cooperation of the Cloud provider, the only mitigation action possible would be to ensure that encryption is used when data are transmitted and/or stored. Note that in such a scenario, the way in which the cryptographic keys are managed is critical and the challenge will be to find solutions that offer the required level of security at a reasonable cost. Security certification[23] of the Cloud Service Provider is now a precondition for a customer and evidence needs to be provided in regular phases.

Privacy Enhancing Technologies (PETs). Cryptographic tools are important defence mechanisms against cyber-attacks, c.f. ENISA's position on Cryptographic tools[24]. While strait forward crypto implementations can protect confidentiality and integrity of data towards outsiders, PETs consider adversaries that play a

[19] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto, accessed April 2017.
[20] https://www.enisa.europa.eu/publications/big-data-security, accessed April 2017
[21] https://www.enisa.europa.eu/publications/big-data-security, accessed April 2017
[22] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view , accessed April 2017
[23] https://resilience.enisa.europa.eu/cloud-computing-certification , accessed April 2017
[24] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption, accessed April 2017

role in a certain service, e.g., we can hide the identity of communication partners from the communication service provider or the search phrase from a database host. Such technologies can increase the trust users have in a given service in a society that increasingly depends on electronic services, which process large amounts of personal data.

However, PETs also have a positive effect on network security by reducing the attack surface. Service Providers that implement PETs can, e.g. minimize the data they need to protect, hence even a successful attack will not gain access to excessive amounts of data. Further, data can be decomposed and distributed in such a way that an adversary needs to compromise several services to recompose data items for a successful attack. Our work on privacy by design helps service providers to implement such mechanisms[25,26].

Incident notification and information/intelligence sharing. It has been already understood that it is important to understand the origin and purpose of security incidents. Incident notification has been part of European regulation in the areas of Telecommunication and since recently in other areas of critical information infrastructures. In the context of Cloud Computing, for example, the NIS Directive extends the provisions of the Telecoms Package[27] to Digital Service Providers (including CSP). Like Article13a in the Telecom sector, Article 15 will impose incident reporting on the cloud providers. National competent authorities, having under their jurisdiction cloud providers, will be established, thus enhancing Cloud security, privacy and resilience across the EU. ENISA is supporting the activities of the proposal, paving the way for a new era in Cloud security.

Incident notification is an important tool towards defending state sponsored activities. Yet, the creation of the necessary holistic view of an attack will be difficult to create. This fact is aggravated by the difficulty of attribution of attacks in cyber-space. In addition to incident notification, sharing schemes will be necessary in order to exchange information and intelligence about cyber-attacks. Given the fully confidential nature of defence of state sponsored attacks, the establishment of information sharing and analysis schemes will be difficult to achieve.

Certification. Even for experts, it might be hard to assess the quality of a crypto product. A number of European legislative initiatives related to information technology have been launched in the recent years. The most relevant of them are the NIS Directive, the General Data Protection Regulation (GDPR), the eIDAS Regulation and the Revised Directive on Payment Services (PSD2). These legal acts rely on the availability of trustworthy information technology products that support the deployment of robust information systems in Europe.

Trustworthiness and security of information technology products can be enhanced by setting in place a certification framework. In Europe, a common scheme would support the recognition of security certification across Member States, an essential pillar towards achieving trust and security required to promote the Digital Single Market. Currently, there is no such framework at European level, although the already existing mechanism SOG-IS includes 10 Member States and Norway.

Conclusion. For another time reality comes to lead taboos of the past ad absurdity: although in the past state sponsored activities have not been seriously considered, in today's digital society state sponsored attacks play a role at the first line of cyber-defence. Fortunately, the defence against such adversaries is no

[25] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, accessed April 2017.
[26] https://www.enisa.europa.eu/publications/pets, accessed April 2017.
[27] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0140 , accessed April 2017

different than from other malicious users. Hence, available know-how on cyber-defence mechanisms are fully capable of defending this cyber-threat.

In the light of the current trends in state sponsored activities, we see the following emerging issues (non-exhaustive, non-prioritised):

- Work on attribution of incidents and recognition of targets/campaigns.
- Coordination of available defence forces.
- Identification of defence strategies tailored to state sponsored activities.
- Identification of necessary synergies and emergency plans towards defending states sponsored attacks.
- Development of guidance for cyber-diplomacy.
- Development of common attack scenarios/methods and their defence.
- Elaborate on the role of cyber-threat intelligence and enforce its use to structure defences.
- Identification of potential cyber-tools and methods portfolios for this types of attacks.
- Elaborate on methods to trace activities of related threat agents and improve attribution of cyber-attacks.
- Revise legal frameworks to accommodate defence activities to state sponsored cyber-attacks.
- Include this kind of attacks to risk and threat assessments.
- Find appropriate options to properly operate and reduce attack surface of existing security controls, in particular regarding encryption and privacy enhancing technologies.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu