ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ

CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

The Greek wiretapping scandal and the false promise of intelligence cooperation in the information era

Vasileios Papageorgiou

Research Paper No. 29

ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

The Greek wiretapping scandal and the false promise of intelligence cooperation in the information era

Vasileios Papageorgiou

Senior Researcher at KEDISA

Research Paper No. 29

Table of contents

List of Abbreviations

ADAE	Hellenic Authority for Communication Security and Privacy
APT	Advanced Persistent Threat
BSC	Base Station Controller
BTS	**(**Cellular) Base Station Transceiver
CEO	Chief Executive Officer
CIA	Central Intelligence Agency (USA)
ETSI	European Telecommunications Standards Institute
EYP	Greek National Intelligence Service
IMS	Interception Management System
IR	International Relations (Field of studies)
LEA	Law Enforcement Agency
LI	Lawful Interception
MI5	United Kingdom Security & Intelligence Service
MSC	Mobile Switching Center
NSA	National Security Agency (USA)
RES	Remote Control Equipment Subsystem
SIGINT	Signals intelligence
SID	Signals Intelligence Directorate
US	United States (of America)

Introduction[1]

A few months after the end of the Olympic Games of 2004, the Greek government revealed a serious wiretapping scandal that started during the Games and continued until early 2015. The wiretap, which was labelled by the media as the "Greek Watergate" (Smith 2006), had on its target more than 100 top Greek officials, including Kostas Karamanlis, the Greek Prime Minister of that time. Even to this day, the identity of the perpetrators remains unknown, as some parts of this case are characterized by considerable ambiguity due to the hybrid nature of the cyber-attack and the involvement of intelligence agencies. Moreover, this case of wiretapping gained much more attention from the media, when it was connected to the suicide of the network-planning manager at Vodafone Greece, the telecommunications company, the software of which had been exploited by the perpetrators with the use of a sophisticated bug. As it was later revealed by the documents leaked by Snowden, the Greek National Intelligence Service (EYP) collaborated closely with the National Intelligence Agency (NSA) of the United States of America (US) and partly with the Central Intelligence Agency (CIA) of the latter, to assist each other in providing security during the Olympics. Consequently, a certain agreement was made between those intelligence agencies based on two fundamental principles. Firstly, the main goal of the operation was to conduct surveillance on certain groups that were possibly linked to terrorism, as indicated by EYP. Secondly, those actions would have taken place only during the Olympic Games and not afterwards. Apparently, neither part of the deal was respected.

The main purpose of this paper is to examine the relation between different national intelligence agencies in the information era. More specifically, it is supported that it is difficult, if not impossible, to establish a trustful relationship between national intelligence agencies, even between allies, when it comes to cooperating and collecting information in foreign soil. Consequently, the case study of the wiretapping scandal in Greece will be a helpful tool in this analysis, given the reason that the cyber capabilities of modern states can be an essential tool for collecting foreign intelligence. The main theory that will be used to examine this idea, is the Realist approach in the International Relations (IR) field of studies. In short, Realism supports that the antagonistic nature of the international system makes it impossible to establish a multinational intelligence cooperation in the long term, since each state will try to exploit the

[1] This analysis is based on a paper written for the MSc Crisis and Security Management, Leiden University.

value of the relevant information in order to protect or to increase their relative advantage (Phythian 2009). Intelligence is, therefore, another tool in the hands of the states, in their struggle for getting more power under a state of anarchy (Munton 2009).

In the first chapter, the main aspects of Realism in relation to the notion of intelligence will be presented. How intelligence cooperation and the notion of intelligence in general are perceived under the spectrum of Realism in IR? In the next chapter, the case study of the Greek Watergate scandal will be presented in detail, from the very beginning. The security concerns, the collaboration between EYP and the NSA, the legal framework of the wiretaps, and some technical aspects of the malware will be discussed. How sophisticated the malware was and how was the procedure carried out? Finally, this chapter will close with presenting the reaction of the Greek government and the possible role of the foreign intelligence services in this scandal. Was Greece's strategy effective in terms of Cyber Security governance? On what grounds can one support that this code was developed by a nation and not by an individual hacker? Did it consist an advanced persistent threat? As a part of this chapter, potential links between the death of the network-planning manager of Vodafone and the wiretapping case will be shortly addressed. Is this case linked to the wiretapping scandal? Is he a likely a victim of intelligence agencies? By the end of this paper we will try to answer these questions, at least to a certain extent, given the ambiguity of the topic. In short, the paper concludes that no relationship based on trust can be established between intelligence agencies in the information era, as Realism suggests.

Last but not least, it is important to define some of the notions that will be used in this paper. Although there are various definitions on intelligence, we will define this notion using the first part of a CIA accepted definition as provided by Bimfort (1958) "Intelligence is the collecting and processing of that information about foreign countries and their agents which is needed by a government for its foreign policy and for national security". Subsequently, intelligence cooperation will be defined using the definition provided by Richelson (1990) as "arrangements by a government to exchange intelligence with a foreign government or permit another nation to establish intelligence facilities on one's territory to yield important benefits". Finally, when it comes to the notion of wiretapping, we will use the definition provided by Arrigo (2014) "wiretapping is one form of electronic eavesdropping and specifically references the monitoring of phone (landline or cellular) conversations by a third party".

Realism in IR and the notion of intelligence

Although various IR theories may be used to define the notion of intelligence, the contemporary literature is dominated by a strong realist perspective (Lillbacka 2013). In a state of anarchy in the international system, the insecurity that every state is experiencing makes cooperation between different states a difficult practice. Unless there is an emergence of a common threat in the international system, according to the basic principles of Realism, "cooperation amongst states is not the norm" (Munton 2009). This perception applies to almost every aspect of Realism. The notion of intelligence seems to follow this norm as well. According to Sir Stephen Lander, former director-general of the United Kingdom Security & Intelligence Service (MI5), as quoted by Munton (2009) "intelligence services and intelligence collection are at heart manifestations of individual state power and of national self-interest" To this extent, intelligence is a zero-sum game, whereas one state's loss is another state's gain. Knowledge is power for one state and thus, effective intelligence is a force multiplier (Munton 2009).

Consequently, intelligence is not merely seeking access to the information of foes, but on certain occasions, aims friendly states as well (Munton 2009). While the periods of the WWII and the Cold War are rich in such practices, even in the post-Cold War era, espionage is also taking place between allies, largely thanks to technology (Martinez 2013). Some contemporary and prominent cases of espionage between allies revealed by the classified documents leaked by Edward Snowden. These documents gave a glimpse of the "modus operandi" of the US intelligence services and their attitude towards intelligence gathering by allies of the US. According to these documents, the NSA targeted among others, the official cellphone of the German Chancellor, Angela Merkel and wiretapped millions of calls by politicians in both Spain and France (Martinez 2013). When the former director of the NSA, James Clapper, was asked about those revelations he underlined that the gathering of intelligence on foreign leaders is a fundamental right for the US (Martinez 2013). This Machiavellian approach seems to conclude the approach of the intelligence agencies regarding intelligence cooperation. Last but not least, this perception of "the ends justify the means" of intelligence services was further enforced by the September 11 attacks.

The Olympic Games of 2004 and the security background

Collaboration between EYP and the NSA/CIA

The Olympic Games of Athens in 2004 was the first major event that took place outside of the US and most importantly, the first event of that scale that was organized after the September 11 terrorist attacks. Concerns about security were intense and the US intelligence services started their preparation for this major event well in advance. According to the documents leaked by Snowden, the preparation started at least two years prior to the Olympics of Athens (National Security Agency - NSA 2003). In a relevant document, the increasingly significant role of the NSA in collecting information during the Olympic Games since 1984 is mentioned in a straightforward way (National Security Agency - NSA 2003). Most notable is however the reference to the Olympics in Athens. As stated in the classified document "NSA's support to the 2004 Olympics in Athens will be much more complicated" (National Security Agency - NSA 2003). One of the most crucial differences from previous likewise operations is the fact that the NSA had to collaborate with the Greek Intelligence Service (EYP), a procedure that would take a lot of preparation according to the NSA (2003). For the reasons above, the NSA (2003), sent the largest group of specialists in their history in support of the games. The conclusion of the report is characteristic "The scope of the Olympics is tremendous, and so will be the support of SID[2] and NSA. The world will be watching, and so will NSA!" (National Security Agency - NSA 2003).

Although the cooperation of the NSA and EYP was intended to be close, there were some frictions between the US and the Greek authorities. Most notable was the technical difficulty of the Greek law enforcement agencies (LEAs) and the limited capabilities of EYP to establish mass surveillance. On the contrary, EYP could only establish surveillance within a very limited distance, which was terrifying from the American point of view (Petropoulos 2015). After significant pressure from the US, the Minister of Public Order in Greece called a meeting in December 2003 among the three cell phone providers of that time, Cosmote, Vodafone and Tim (Petropoulos 2015). The aim of the meeting was to discuss how Lawful Interception (LI) could

[2] Signals Intelligence Directorate (SID), is an important division of the NSA, primarily responsible for the collection, analysis, production and dissemination of SIGINT data (telecoms, fax, telegrams, etc).

be implemented. However, the general elections that were scheduled for the upcoming March, made it impossible to issue the presidential decree needed. Even after the change in government, no legal framework was in place a few days before the beginning of the Olympics (Petropoulos 2015).

The Lawful Interception security process

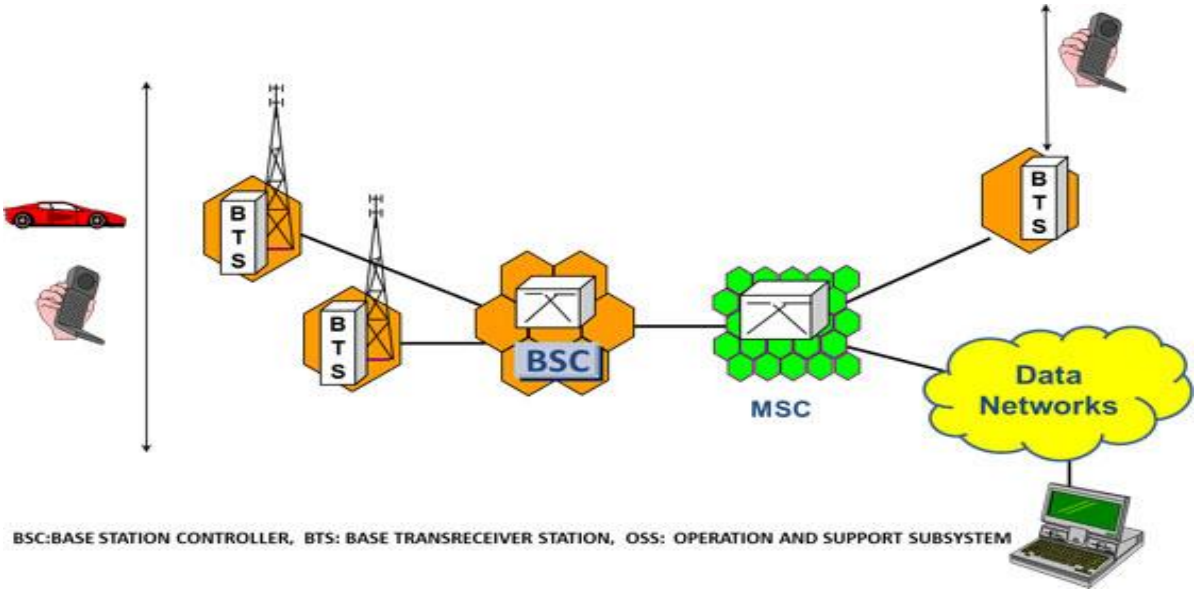
Despite the problems with the legislation, a code of 6500 lines of illegal software was added (officially by unknown perpetrators) in the source code of the software used by Vodafone Greece to operate its network. It was the 4th of August 2004, approximately 10 days before the opening ceremony of the Summer Olympic Games (Petropoulos 2015). The developer of the main software of Vodafone was Ericsson, the prominent Swedish tech company (Bamford 2015). The latter, "handed" an upgrade to Vodafone containing the Lawful Interception program. According to the European Telecommunications Standards Institute (ETSI), Lawful Interception (LI) is a "a security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organizations". Subsequently, as Law Enforcement Agencies (LEAs) are defined the "services authorized by law to carry out telecommunications interceptions." (Council Resolution of 17 January 1995 on the lawful interception of telecommunications 1995). It can be therefore concluded that, when adopted under normal legal circumstances (warrant from a LEA), LI is a permitted and legal procedure under the Greek (*ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3115 (ΦΕΚ Α΄ 47/27-2-2003) Αρχή Διασφάλισης Του Απορρήτου Των Επικοινωνιών* 2003) and the EU (96/C 329/01) law.

Nevertheless, in the abovementioned update by Ericsson, in early 2003, a specific software subsystem was included, known as the "Remote Control Equipment Subsystem" (RES) (Prevelakis and Spinellis 2007). The RES can copy a conversation of a targeted, wiretapped phone into a second stream and normally, send this copy to Law Enforcement Agencies (Romanidis 2008). Ericsson optionally provides an Interception Management System (IMS) with the use of which the LI can be managed by the operators after a relevant court order. Any wiretap in the RES without a relevant request for a tap in the IMS software is a good indicator that an unauthorized tap has taken place (Prevelakis and Spinellis 2007). It is now known that Vodafone had not activated the LI option, nor had the company installed the IMS software by that time. However, after the update of 2003, the code (RES) was introduced to the software of

Vodafone, without, though, the IMS, which is normally used as the interface in such occasions (Romanidis 2008). Consequently, the hackers exploited this feature by adding a highly sophisticated bug in the source code of Vodafone.

The sophisticated bug

In order to understand this rogue operation, it is essential to briefly present the common, basic cellular structure which mostly remains the same in most countries during the last decades. In short, during a telephone call, the voice is transmitted in the form of digital data to a transceiver at a nearby cellular base station (BTS). In this station, the base station controller (BSC), in other words, a special computer, delivers radio channels and coordinate handovers among the transceivers under its authority (Prevelakis and Spinellis 2007). The BSC then achieves communication with a mobile switching center (MSC) which in turn connects the phone calls to the desired end-users, such as call recipients of the same switching center, or other switching centers, up to foreign networks (Prevelakis and Spinellis 2007). In the following diagram the basic cellular architecture is presented. The cells represent the coverage and the capacity of the network, in area and subscribers respectively.



Source: *Cellular Operators Association of India*

The bug required indeed a very deep knowledge of the Vodafone network and the Ericsson source code (Petropoulos 2015). Among others, the perpetrators managed to install and operate the illegal software for months, without being detected by Vodafone or Ericsson. More specifically, the hackers successfully implanted the rogue software in four MSC of Vodafone

(Romanidis 2008). As the MSCs were located in the heart of the mobile phone network, they were the main target of the intruders (Prevelakis and Spinellis 2007). But without the IMS interface as stated above, where did the second recorded stream ended? According to a 2011 investigation conducted by the Hellenic Authority for Communication Security and Privacy (ADAE), 14 shadow-phones located in various places in the city of Athens, were used as transceivers of the voice data (Petropoulos 2015). Unlike the highly sophisticated code that was used for the hacking, the wiretapping procedure was straightforward, however invisible to Vodafone. As a result, it seemed that the exploitation of RES for certain phone numbers as well as the simultaneous erase of any tracks that could reveal the presence of the illegal software and the perpetrators, underlined the success of that cyber-attack and apparently the whole wiretapping (Prevelakis and Spinellis 2007).

Indications of a possible cyber-intervention in the software of Vodafone were found accidentally, on January 24, 2005, when the perpetrators updated the rogue software. This lead to a malfunction in the system regarding the delivery of text messages and as a result, thousands of complains were made by Vodafone's subscribers. Immediately, the company asked the help of Ericsson to investigate the problem. After numerous checks, Ericsson technicians informed Vodafone that traces of unauthorized software were found and further isolated the malware in Ericsson Headquarters in Sweden (Petropoulos 2015). On Tuesday, the 8th of March, Vodafone's CEO, Giorgos Koronias, ordered technicians to deactivate and erase the malware from Vodafone's network (Prevelakis and Spinellis 2007). By doing so, the Greek authorities missed any opportunity they had to find the perpetrators by spotting the location of the shadow phones (Prevelakis and Spinellis 2007).

The revelation of the wiretapping scandal and the role of foreign intelligence services

The reaction of the Greek Government and the Greek authorities

On March 10, 2005, the CEO of Vodafone Greece, asked for a meeting with the Prime Minister, Kostas Karamanlis to discuss the wiretapping issue. Since the latter was not in Greece, a meeting between Koronias and the Minister of Public Order, Giorgos Voulgarakis, was scheduled instead (Petropoulos 2015). On the same day, the decree that was making the

wiretaps legal, and was missing before and during the Olympics, was published in the Government's Gazette (Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας 2005 & Petropoulos 2015).

It seemed that the Greek government who agreed to the conduction of wiretaps by the NSA in close collaboration with EYP, never ensured that this procedure really ended once and for all (Petropoulos 2015). Under the burden of this scandal, the initial thought of the Greek government was to bury the whole case. However, Kostas Karamanlis dismissed that plan, upon the fear that the case would be leaked at a later date (Petropoulos 2015). While the issue was under investigation from the Greek authorities, the ADAE, the legal authority with technical expertise, was never informed about the incident (Petropoulos 2015). It was not before February 2006, when the Minister of Public Order, the Minister of the State, and the Minister of Justice, held a press conference, informing the public that a total of 105 phones were wiretapped, including phones of top officials like the Greek Prime Minister Kostas Karamanlis and his wife, other Ministers and prominent journalists in Greece (Μανδραβέλης 2008). The most outrageous and controversial moment during the press conference was the praise of the Minister of Public Order towards the CEO of Vodafone, for its handling of the situation. The press conference ended by admitting that a total of 11-month investigations had not provided any sufficient evidence to the authorities about the identity of the perpetrators (Petropoulos 2015).

The biggest question of who was the human factor that might carried out the operation remained without any answer for years, till February 2015, when the Greek authorities issued an international arrest warrant for a CIA official, named William George Basil (Bamford 2015). That step was "a nearly unprecedented action" by an allied country such as Greece, as an intelligence official of the US was accused of espionage and the violation of privacy laws. This case, however, did not gain any attention in the US media (Bamford 2015). According to the magistrate that issued the warrant, the evidence lies on the fact that the wife of Basil bought the shadow phones that were used for the wiretapping, on his behalf (Petropoulos 2015). Moreover, the investigation of the ADAE showed direct links between some of the abovementioned shadow phones with the US embassy in Athens (Bamford 2015). On the other side of the Atlantic though, the US seem to downplay the importance of the issue, and therefore ignore the warrant issued by the Greek authorities. Last but not least, the Vodafone's company was fined with an initial 76 million euros fine (it was later converted to a 50m one) for their mismanagement in this case by the ADAE ("Πρόστιμο 50 Εκατ. Ευρώ Επέβαλε Εκ Νέου Η ΑΔΑΕ Στη Vodafone" 2013).

An Advanced Persistent Threat (APT) by foreign intelligence services?

Even to this day, this code of 6500 lines is considered to be a technological and methodological reference point. It can be thus added that this malware falls under the category of threats that are known in the relevant bibliography as "Advanced Persistent Threats" (APT). It's not easy to briefly define what an APT attack is. Therefore, we will note the main characteristics that an attack needs to possess in order to be characterized as an APT. Those are, namely, the sophisticated nature of the attack, its targeted scope, the systematic effort to find a system's vulnerability by the perpetrators, adaptation of the attackers to any security measures while escaping detection for a considerable period and finally, the use of multiple attack vectors (IMT4582 Network security 2013). Considering the abovementioned criteria, one could argue that the case of Greek wiretapping is possible to be recognized as an APT. The whole operation was indeed a sophisticated, targeted, systematic effort (considering the 6500 lines of code) that was unnoticeable for months with the use of multiple vectors (cyber but also physical since someone who had access uploaded and maintained the illegal software).

Considering the above, it can be argued that there are some noticeable similarities with the notorious Stuxnet malware, perhaps the most famous example of APT till today. As most of the malware created by individual hackers have imperfections on their codes, in the case of Stuxnet, the structure of the code was indeed written in a thorough and professional fashion. This perfection suggests that the malware was the outcome of an orchestrated and continuous effort that required a considerable number of tests before the release of the malware in the targeted systems, and thus it required capabilities that can only be compared with the capabilities that a state possess (IMT4582 Network security 2013). Although Stuxnet remains until today probably the most notorious malware that humanity ever witnessed, the code of the 6500 lines installed in Vodafone's software resembles to Stuxnet at least to a certain extent. More specifically, the basic similarities are the sophisticated way that the code was constructed and the long time that it remained practically unnoticeable by the technicians in Vodafone Greece. Consequently, suspicions fall on the NSA for orchestrating this case of wiretapping since it definitely possessed the capabilities for such an act.

The involvement of the intelligence services of the US in this kind of operations and in particular foreign intelligence services like the NSA, is evident. The interest that the NSA had on the LI procedure is underlined by a power point presentation classified as a "top secret", regarding the exploitation of the LI procedure (S31122, n.d.). In the same document, it is presented that the NSA possessed the capability to identify approximately 60 "fingerprints"

(ways to identify data) from various companies which developed lawful interception subsystems, including Ericsson (S31122, n.d.). According to another leaked document, a highly talented group of hackers of the NSA, actively participated during the involvement of the latter in the Summer Olympics of Athens (National Security Agency - NSA 2003). As a final confirmation of the involvement of the US foreign intelligence service in this operation, a former official of the US intelligence openly admitted on 2015 that the operation was carried out by the NSA, with the consent of the Greek government, at least during its initial stages (Petropoulos 2015). According to the same official, who asked not to be identified, during his interview in the Kathimerini newspaper "The Greeks identified terrorist networks, so NSA put these devices in there and they told the Greeks, "OK, when it's done we'll turn it off [..]"" (Bamford 2015). As a conclusion, it seems that the Greek intelligence services and the Greek government rested on that promise.

A likely casualty of the intelligence services?

The fact that gave an even bigger extent to the wiretapping scandal and might be linked to this eavesdropping scandal, is the suicide of Vodafone's leading software engineer, Costas Tsalikides, on the 9th of March 2005, just a day after his boss (the CEO of Vodafone Greece) ordered the removal of the illegal software (Bamford 2015). Costas Tsalikides seemed to be indeed deeply involved in the notorious case. He, the network-planning manager, had already noticed some problems in the previous months by observing that certain antennas seem to overwork and as a result they became overheated. It was actually true that those antennas were indeed connected to the wiretapping, as it became evident at a later date (Bamford 2015). In addition to that, according to a report released by ADAE in 2011, the Vodafone employee who accepted the delivery of the upgrade of the malware on January 24, 2005 was Costas Tsalikides (Bamford 2015). It seemed that the network-planning manager had realized that something suspicious was going on in Vodafone. A few days before his suicide, he told his fiancée that leaving Vodafone was "a matter of life and death" (Petropoulos 2015). Consequently, Costas handed his resignation on the 31st of January 2005 to his supervisors, who instead persuaded him to stay in the company until they could find a replacement. The night that the code was removed from the Vodafone's software was the last night that he gave life signs. In the following morning, he was found by his brother in his apartment in Kolonos (Athens) hanging down from a rope above his bathroom door (Bamford 2015).

According to his relatives, Costas profile did not match the profile of a person likely to commit suicide. On the contrary, the family of Costas as well as the public in Greece and the worldwide media, hold the belief that he was a likely victim of intelligence agencies as he may have as well discovered the identity of the perpetrators due to his position (Smith 2006). Under a Realist perspective and taking into consideration some empirical data from the history of the intelligence services, this would not be an unlikely scenario. Intelligence is one of the most sensitive and sovereign elements of a country. In ensuring national interest, intelligence agencies have often adopted a Machiavellian approach in order to achieve their ends. It has to be noted though, that up to this day, even though there are some indications that the death of Costas Tsalikides was not a mere coincidence and maybe even not a suicide, there are is no sufficient evidence to prove that hypothesis or to directly accuse any foreign intelligence service.

Conclusion

To conclude, the wiretapping scandal in Greece raised plenty of questions about the role of intelligence agencies, their collaboration with other national intelligence services and the cyber capabilities that they possess and exploit in states with narrower relevant capabilities. In the past, collecting intelligence was a difficult and long procedure. In the information era though, intercepting communications is way easier by hacking the telecom provider. Although due to the hybrid nature of the attack, certain parts of this case remain blurred, according to the analysis conducted and under the prism of Realism, our thesis is confirmed. Intelligence cooperation does not seem to be taking place in a win-win base, but instead, an antagonistic philosophy characterizes the struggle for information by intelligence agencies. Although the relation between the US and Greece seem to be admittedly friendly, there are strong indications that the intelligence services of the former exploited the opportunity of conducting wiretaps and therefore espionage to top Greek officials since they possessed this (cyber) capability. As a result, the US intelligence agencies broke their initial agreement with the Greek government and the Greek National homologous services, and conducted the wiretapping under the nose of EYP.

As unequivocally stated by prominent intelligence officials and as seen by the case study of Greece (2004-2005), wiretaps are a widespread practice between allies, making intelligence

cooperation only partly feasible and risky for the ones involved. The Greek case study is a characteristic example of the above. More specifically, the Greek government handled poorly the case in terms of Cyber Security governance, by giving the NSA almost full authorization to commence and monitor the LI procedure and without even properly changing or checking the software's code by the end of the games. Moreover, while there are some indications that the death of Costas is linked to the wiretapping scandal this is not yet confirmed and it is unlikely to be soon, given that there is no sufficient evidence due to the nature of the case. On the contrary, the cynical approach of intelligence agencies when it comes to collecting intelligence seems to be crystal clear. Quoting an ex-member of the NSA with experience in wiretapping "They never remove (the bugs). Once you gain access, you are in. You have the chance to put in (more) bugs, and this is an opportunity".

References

Primary Sources

Council Resolution of 17 January 1995 on the lawful interception of telecommunications. 1995 (96/C 329/01). COUNCIL OF THE EUROPEAN UNION.

National Security Agency - NSA. 2003. "(U//FOUO) NSA Team Selected for Olympics Support". NSA Olympics Support Team.

National Security Agency - NSA. 2003. "(U//FOUO) SID Trains for Athens Olympics". USAF SIGINT Communications.

National Security Agency - NSA. 2004. "(U) Another Successful Olympics Story". Collection Strategies and Requirements Center (S3C).

National Security Agency - NSA. 2004. "(U) Gold Medal Support to The Summer Games". Link Access Programs (S33).

S31122, National Security Agency. n.d. "(S//SI//REL) Exploiting Foreign Lawful Intercept (LI) Roundtable". Presentation.

Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας. 2005. "Εφημερίς Της Κυβερνήσεως Τεύχος Πρώτο". Αθήνα: Εθνικό Τυπογραφείο.

ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3115 (ΦΕΚ Α΄ 47/27-2-2003) Αρχή Διασφάλισης Του Απορρήτου Των Επικοινωνιών.. 2003. Vol. 1. Athens: Υπουργείο Δικαιοσύνης.

Secondary Sources

"Lawful Interception". 2017. *ETSI*. Accessed October 17. http://www.etsi.org/technologies-clusters/technologies/lawful-interception.

"Πρόστιμο 50 Εκατ. Ευρώ Επέβαλε Εκ Νέου Η ΑΔΑΕ Στη Vodafone". 2013. *Kathimerini.Gr*. http://www.kathimerini.gr/477082/article/oikonomia/epixeirhseis/prostimo-50-ekat-eyrw-epevale-ek-neoy-h-adae-sth-vodafone.

Arrigo, Bruce A. 2014. *Encyclopedia of Criminal Justice Ethics*. 1st ed. Charlotte: SAGE Publications.

Bamford, James. 2015. "Did A Rogue NSA Operation Cause the Death Of A Greek Telecom Employee?". *The Intercept*. https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/.

Bimfort, Martin T. 1958. *A Definition of Intelligence*. 2nd ed. CIA HISTORICAL REVIEW PROGRAM.

IMT4582 Network security. 2013. "Advanced Persistent Threat (APT) Beyond the Hype". Gjovik University College.

Martinez, Michael. 2013. "Allies Spy On Allies Because Friends Today May Not Be Friends Tomorrow - CNN". *CNN.Com*. http://edition.cnn.com/2013/10/30/us/spying-on-allies-everybody-does-it/index.html.

Munton, Don. 2009. "Intelligence Cooperation Meets International Studies Theory: Explaining Canadian Operations in Castro's Cuba". *Intelligence and National Security* 24 (1): 119-138. doi:10.1080/02684520902756960.

Petropoulos, Aggelos. 2015. "Americans And Greeks Started The 2004 Wiretaps Together". *Ekathimerini.Com*. http://www.ekathimerini.com/202026/interactive/ekathimerini/special-report/americans-and-greeks-started-the-2004-wiretaps-together#secondPage.

Phythian, Mark. 2009. "Shared World or Separate Worlds? International Theory and Theories of International Relations". In *Intelligence Theory, Key Questions and Debates*, 2nd ed. Abingdon: Routledge.

Prevelakis, Vassilis, and Diomidis Spinellis. 2007. "The Athens Affair". *IEEE Spectrum* 44 (7): 26-33. doi:10.1109/mspec.2007.376605.

Richelson, Jeffrey T. 1990. "The Calculus of Intelligence Cooperation". *International Journal of Intelligence And Counterintelligence* 4 (3): 307-323. doi:10.1080/08850607.2013.732450.

Romanidis, Evripidis. 2008. "Lawful Interception and Countermeasures". Master, Royal Institute of Technology Stockholm, Sweden.

Smith, Helena. 2006. "Death of Vodafone Engineer Linked To Greek Watergate". *The Guardian*. https://www.theguardian.com/business/2006/jun/23/city.mobilephones.

Μανδραβέλης, Β. 2008. "Πώς Ο «King George» Έχασε Τον Θρόνο Του Στη Vodafone Μετά Τις Τηλεφωνικές Υποκλοπές, Του Β. Μανδραβελη | Kathimerini". *Kathimerini.Gr*. http://www.kathimerini.gr/314410/article/oikonomia/epixeirhseis/pws-o-king-george-exase-ton-8rono-toy-sth-vodafone-meta-tis-thlefwnikes-ypoklopes.