MOL2NET 2017, International Conference on Multidisciplinary Sciences, 3rd edition. Section 08: LAWSCI-01: Wokshop on Challenges in Law, Technology, Life, and Social Sciences. 25 – 30 July, 2017. Bilbao, Spain.

WORLDWIDE CYBER-ATTACKS: THEIR IMPACT ON THE INTERNATIONAL HEALTH SERVICES AND THEIR ANSWER IN THE SPANISH CRIMINAL CODE

Iker Conal

Chair in Law and the Human Genome Research Group

University of the Basque Country (UPV/EHU), Barrio Sarriena, s/n, Leioa (Biscay), 48940

Tlf.: 946012000. Email: iker.conal@ehu.eus

Abstract

On 12th May 2017, many health services around the world suffered the attack of the "WannaCry" ransomware. This paper exposes the main consequences faced by them in the United States, Great Britain, Germany, Australia, New Zealand and Spain, and the possibilities according to the Spanish Criminal Code of prosecuting this kind of crimes, demonstrating that we must secure the internal excellence of each individual health service, promote the development of new, more technical articles in the mentioned legal text and, above all, strengthen the international cooperation in order to effectively prosecute these attacks.

Keywords: cyber-attack; international; health; services; criminal; prosecution.

1. INTRODUCTION

Imagine the nearest hospital to your home. Suddenly, a telephone rings and a known but nervous voice gives a strange and urgent order: *"A massive cyber-attack is damaging our system. Switch off all the computers. All of them. Immediately!"*

You obey the command but, at the same time, you start asking yourself an infinite amount of questions; how is the health system going to work? What will happen with the patients? Is this action really *legal*? Is someone going to prosecute the authors of the attack? This paper tries to answer some of these questions. Information is the key to

understand what some authors have called the biggest massive cyber-attack in history[1], even more if we take into account that the day the attacks took place the confusion among the citizenry was absolute until the authorities started clearing the situation.

The virus "WannaCry" has been considered by Europol as unprecedented: it blocked the computer systems of hundreds of companies and institutions in more than 70 countries, affecting more than 200,000 computers. Thanks to this tool, the criminals developed a massive campaign of "ransomware", demanding money (the so called "bitcoins", a digital coin difficult to track) to the victims in exchange of the access to their systems. If we pay attention to the opinion of the most prestigious jurists[2], it is undeniable that these actions reunite all the requirements to be considered as criminal activities.

2. THE IMPACT ON THE INTERNATIONAL HEALTH SERVICES

According to experts[3], the "WannaCry" infection, in a hospital setting, is able to cause a block in the access to lab results or patient records, or even a failure to share drug interaction or allergy information between hospital computers or other devices. The most important element here is *centralization*. Indeed, it may have been the reason why hospitals and other medical organizations in the United States avoided serious damages (although the American systems got impacted in some regard): they are less centralized than the British one. However, American health care providers are worried, as we can see in one large hospital system in Boston, where all attachments in e-mails have been disabled and they prepare themselves for hypothetical future attacks.

When it comes to health services, the country that has suffered the biggest damage is, without any doubt, the United Kingdom, which has one of the most centralized health care systems in the world. The state-run National Health Service (NHS) declared a major

---

[1] P.A. Navarro, "Terror en el ciberespacio: El mayor ataque coordinado a ordenadores de medio mundo desata las alarmas", *El Siglo de Europa,* no. 1.201, 2017, http://www.elsiglodeuropa.es/siglo/historico/2017/1201/Index%20Los%20Dossieres.html (accessed 20 July 2017)

[2] C.M. Romeo Casabona, "De los delitos informáticos al Cibercrimen", in F. Pérez Álvarez (ed.), *Universitas Vitae. Homenaje a Ruperto Núñez Barbero*, Salamanca, Ediciones Universidad de Salamanca, 2007, p. 650. *"Por otro lado, también pueden realizarse modificaciones, incluso meramente transitorias, de datos o de sistemas informáticos con el fin de inutilizarlos o de obtener un beneficio, por lo general económico. Son, asimismo, demasiado conocidas las difusiones de virus informáticos a través de la red, los cuales suelen expandirse con gran rapidez y amplitud en todo tipo de terminales […], pudiendo alcanzar sus daños globales en ocasiones cuantías económicas muy elevadas".* We can find early references to this kind of crimes in C.M. Romeo Casabona, *Poder informático y seguridad jurídica: la función tutelar del derecho penal ante las nuevas tecnologías de la informática*, Madrid, FUNDESCO, 1987. In the last section of this paper we´ll analyse if the Spanish Criminal Code punishes this kind of actions, and how. Whether there´s no doubt of its criminal nature, the question of the legal text preventing this kind of activities is a matter of the highest transcendence in order to pursue them effectively.

[3] D.F. Maron, "U.S. Hospitals Not Immune to Crippling Cyber Attacks", *Scientific American,* May 15, 2017, https://www.scientificamerican.com/article/u-s-hospitals-not-immune-to-crippling-cyber-attacks/, (accessed 22 July 2017). The article shows the high vulnerability of the hospitals and medical devices in the United States.

incident, forcing hospitals to act immediately in order to protect themselves from the attack. In Britain, the NHS was the worst hit[4]. The name of the malware used in their case was "Wanna Decryptor", and it forced staff to use pen and paper again due to the unavailability of key systems, including telephones. NHS organisations across England reported IT failures, and hospitals were forced to turn away patients and cancel appointments, while people in affected areas were advised to seek medical care only in case of emergency. In England, the attack had life and death consequences[5]: the IT systems were shut down in order to protect them, so all systems were offline and hospitals were unable to accept incoming calls. Scheduled appointments had to be cancelled, ambulances were diverted and some departments shut down entirely. Staff did not have access to any digital file. Of course, the NHS had been hit by such attacks before, but this attack has been considered by far the worst.

Germany did not suffer great damages, because its 2,000 hospitals are run by various organizations and, as a consequence, its hospital landscape is extremely decentralized[6]. Australia and New Zealand saw no impact at all in their health systems[7].

In Spain, one of the first countries to suffer the attack, the CCN (Centro Criptológico Nacional), assigned to the CNI (Centro Nacional de Inteligencia), immediately alerted of the attacks. Thanks to this warning, institutions like the Basque Government put into practice their own "active alert", a security protocol oriented to protect, among others, Osakidetza (the Basque Health System)[8]. The answer to the attack consisted in cutting off internet access and blocking access to the email accounts[9]. The damages suffered in the Basque Country were really low, but the Basque Government started working immediately and only

[4] C. Graham, "NHS cyber attack: Everything you need to know about biggest ransomware offensive in history", *The Telegraph,* 20 May 2017, http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/, (accessed 23 July 2017). The ransomware demanded payments of $300 to $600 to restore access. According to this article, Hospitals and GP surgeries in England and Scotland were among at least 16 health service organisations hit by the ransomware, with reports potentially dozens more were affected.

[5] A. Griffin, "NHS cyber attack: Large scale hack plunges hospitals across England into chaos", *The Independent*, 12 May 2017, http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hospitals-hack-england-emergency-patients-divert-shut-down-a7732816.html, (accessed 23 July 2017).

[6] M. Telgheder, "Hospitals Brace for Cyber Attack", *Handelsblatt Global*, 11 July 2017, https://global.handelsblatt.com/companies-markets/hospitals-brace-for-cyber-attack-796113, (accessed 24 July 2017). Prior to "WannaCry", two out of three German hospitals had already been the victims of cybercrime.

[7] Reuters, "Australia and NZ largely escape global cyber attack", *Reuters,* 15 May 2017, http://www.reuters.com/article/cyber-attack-australia-idUSL4N1IG0UI, (accessed 24 July 2017).

[8] J. García, "Un ciberataque especialmente virulento provoca el pánico a nivel mundial", *Deia,* 13 May 2017, http://www.deia.com/2017/05/13/sociedad/estado/un-ciberataque-especialmente-virulento-provoca-el-panico-a-nivel-mundial, (accessed 25 July 2017). Ransomware attacks (on a lower scale) had been suffered in Bilbao.

[9] Agencia EFE, "Las instituciones vascas cierran sus cuentas de correo por precaución tras el ciberataque", *El Correo,* 12 May 2017, http://www.elcorreo.com/bizkaia/tecnologia/201705/12/instituciones-vascas-cierran-correos-20170512194748.html, (accessed 25 July 2017). The internal services kept on track during the attacks.

a month later it announced[10] the creation of a whole new Basque Center for Cibersecurity in ongoing coordination with the Ertzaintza (the police force from the Basque Country) and other institutions.

3. THE ANSWER IN THE SPANISH CRIMINAL CODE

First of all, it is important to understand that is really difficult to catch this kind of criminals due to the nature of the crime itself. We can summarize it in the following terms: the criminals, exploiting a vulnerability in the Windows operating system, send the "ransomware" (a type of malware that encrypts a user´s data, in our case, "WannaCry") to the victims, and then demands payment in exchange for unlocking the data. The criminals demand the payment through cryptocurrency (Bitcoin), and warn that the payment will be raised after a certain amount of time. "WannaCry" does not distinguish between a computer, smartphone or medical device, and there is no need to click a link: if a health care system is connected to the internet and its system is outdated, the malware can find it and infect it. Unfortunately, we will not find this exact (or similar) action in the Spanish Criminal Code, neither a special legislation nor a court to judge it.

However, if we were able to identify the authors and know the place where the actions took place, we could prosecute them in their own countries. In Spain, the cases related to ransomware have been judged[11] as concurrent offences, the addition of a crime of fraud (article 248 and successive of the Spanish Criminal Code) and a crime of damage to computers (article 264 and consecutives of the same legal text).

In conclusion, I think that we must work in three different fields. First, we must guarantee the internal excellence of the health service securing that the last technical updates and security protocols are instituted. Second, we should study the possibility of developing new and more technically accurate articles in the Spanish Criminal Code with the collaboration of the most renowned computer experts. Third, it is imperative to strengthen the international collaboration, like Europol announced days after the attacks, when they started a complex international investigation in order to identify their authors. Only this way we will be able to secure the rights of the most important individuals of the international health service: the patients, guaranteeing their health and wellness.

---

[10] B. Sotillo, "Euskadi se prepara para hacer frente a amenazas y ataques de ciberseguridad", *Deia,* 16 June 2017, http://www.deia.com/2017/06/16/sociedad/euskadi/euskadi-se-prepara-para-hacer-frente-a-amenazas-y-ataques-de-ciberseguridad?random=392666, (accessed 26 July 2017).

[11] A. Ecija Bernal, "Respuestas al ciberataque que ha paralizado España", *Cinco Días,* 12 May 2017, https://cincodias.elpais.com/cincodias/2017/05/12/legal/1494614621_922741.html, (accessed 30 July 2017).

4. BIBLIOGRAPHY

Agencia EFE, “Las instituciones vascas cierran sus cuentas de correo por precaución tras el ciberataque”, *El Correo,* 12 May 2017, http://www.elcorreo.com/bizkaia/tecnologia/201705/12/instituciones-vascas-cierran-correos-20170512194748.html, (accessed 25 July 2017)

Ecija Bernal, A., “Respuestas al ciberataque que ha paralizado España”, *Cinco Días,* 12 May 2017, https://cincodias.elpais.com/cincodias/2017/05/12/legal/1494614621_922741.html, (accessed 30 July 2017)

García, J., “Un ciberataque especialmente virulento provoca el pánico a nivel mundial”, *Deia,* 13 May 2017, http://www.deia.com/2017/05/13/sociedad/estado/un-ciberataque-especialmente-virulento-provoca-el-panico-a-nivel-mundial, (accessed 25 July 2017)

Graham, C., “NHS cyber attack: Everything you need to know about biggest ransomware offensive in history”, *The Telegraph,* 20 May 2017, http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/, (accessed 23 July 2017)

Griffin, A., “NHS cyber attack: Large scale hack plunges hospitals across England into chaos”, *The Independent*, 12 May 2017, http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hospitals-hack-england-emergency-patients-divert-shut-down-a7732816.html, (accessed 23 July 2017)

Maron, D.F., “U.S. Hospitals Not Immune to Crippling Cyber Attacks”, *Scientific American,* May 15 2017, https://www.scientificamerican.com/article/u-s-hospitals-not-immune-to-crippling-cyber-attacks/, (accessed 22 July 2017)

Navarro, P.A., “Terror en el ciberespacio: El mayor ataque coordinado a ordenadores de medio mundo desata las alarmas”, *El Siglo de Europa,* no. 1.201, 2017, http://www.elsiglodeuropa.es/siglo/historico/2017/1201/Index%20Los%20Dossieres.html (accessed 20 July 2017).

Reuters, “Australia and NZ largely escape global cyber attack”, *Reuters,* 15 May 2017, http://www.reuters.com/article/cyber-attack-australia-idUSL4N1IG0UI, (accessed 24 July 2017)

Romeo Casabona, C.M., “De los delitos informáticos al Cibercrimen”, in F. Pérez Álvarez (ed.), *Universitas Vitae. Homenaje a Ruperto Núñez Barbero*, Salamanca, Ediciones Universidad de Salamanca, 2007, pp. 649 – 670.

Romeo Casabona, C.M., *Poder informático y seguridad jurídica: la función tutelar del derecho penal ante las nuevas tecnologías de la informática*, Madrid, FUNDESCO, 1987.

Sotillo, B., “Euskadi se prepara para hacer frente a amenazas y ataques de ciberseguridad”, *Deia,* 16 June 2017, http://www.deia.com/2017/06/16/sociedad/euskadi/euskadi-se-prepara-para-hacer-frente-a-amenazas-y-ataques-de-ciberseguridad?random=392666, (accessed 26 July 2017).

Telgheder, M., “Hospitals Brace for Cyber Attack”, *Handelsblatt Global*, 11 July 2017, https://global.handelsblatt.com/companies-markets/hospitals-brace-for-cyber-attack-796113, (accessed 24 July 2017)