CROSSROADS EUROPE

UACES Student Forum Blog

Archive | Article No 15
Published: 17 August 2017

Permalink: http://uacessf.ideasoneurope.eu/2017/08/17/article-15

Harmful Cyber Operations in the EU: Implementing the NIS Directive into the UK Legal System

Author(s): Eva Saeva

Publication resulting from the UACES 2017 PhD and ECR Conference

*The prevalence of cybersecurity threats against state infrastructure demonstrates the need for an effective European and national response, writes **Eva Saeva**. Focusing on the UK, she argues that, while legal measures are important, the fast-changing nature of the situation means that other avenues, such as public-private cooperation, are also essential.*

The first major cyberattack on a nation state occurred ten years ago, in Estonia in 2007. The attack uncovered a grey area in the field of international law, and policy-makers and security experts were caught off guard.

In the years to follow, malicious activity exploiting the virtual space's endless possibilities and vulnerabilities rapidly evolved and attacks on critical infrastructure increased significantly (e.g. in Georgia in 2008, the Stuxnet worm in Iran in 2010), creating a whole new domain of war – the online borderless world of cyberspace. But international law followed suit and scholars, decision-makers and even the UN agreed that existing international law applies to cyberspace and any comparison with the 'Wild West' was deemed as groundless.

Regardless, many questions remained unanswered. For instance, what *actually* constitutes a harmful cyber operation and *who* can perform such a powerful attack? The term 'harmful cyber operation' means any malicious activity that targets critical infrastructure sectors (e.g. electric grids, nuclear power plants, air traffic control, hospitals, etc.) of another state that can cause major damage, death or destruction in the physical world.

This can be conducted by a group sponsored by a state, or a non-state actor, acting independently. While these attacks might not always cross the threshold of *use of force* (prohibited by Article 2(4) of the UN Charter), they can still cause major consequences for the victim state and violate its sovereignty or the principle of non-intervention.

The European Union has not been immune from these developments. In the EU, cyberattacks (both harmful and non-harmful) against government institutions and critical infrastructure have significantly increased in recent years (e.g. in Italy in 2014, in Germany in 2016, and most recently, in a number of EU countries with the WannaCry ransomware).

Legislation on the malicious use of the virtual space at national level is different in all Member States. However, due to the interconnected information and network systems, an

attack against one Member State will likely have a spill-over effect that could lead to breaching the security of the whole EU. Therefore, the need for a supranational legislation on cyberspace is clear.

As a result, after years of negotiations on promoting closer cooperation on issues such as data protection laws and the internal security of the Union, the Network and Information Security (NIS) Directive, the first comprehensive EU cybersecurity legislative instrument, entered into force in August 2016. It aims at harmonising and stabilising the level of cybersecurity across the Union through public-private cooperation.

The urgent need for such cooperation reflects the awareness that critical infrastructure sectors are mainly managed by private businesses (or 'operators of essential services', as per the NIS Directive) with their own rules and regulations. If states want to achieve a certain level of cybersecurity, public and private actors need to start cooperating more.

Case study: The UK

The UK represents an interesting case for analysis, mainly because of its approach to cyber issues: cyber has been considered a Tier One threat to national security since 2010. In light of Brexit, many will wonder whether or not the implementation of the NIS Directive into national law will happen. The answer is yes. The transposition has to be completed by May 2018, which means that the UK will have to do it regardless of Brexit.

Whether a new law will be introduced or present legislation will be adapted is still unclear. And while in many states the NIS Directive will fill in a void, this is not entirely the case with the UK. Although there is currently no Cybersecurity Act, the UK is one of the states with *some* cyber-related legislation regulating the security and intelligence agencies' work, specifically the Government Communications Headquarters (GCHQ), which deals with cyber issues.

The law currently in force is the Investigatory Powers Act (IPA) 2016, which legalised bulk equipment interference powers, previously known as computer network exploitation and today known as hacking. In other words, the IPA legalised what has already been stated in the National Cyber Security Strategy 2016 – that the UK is developing offensive cyber capabilities.

The recent WannaCry global ransomware attack and its impact on the UK's National Health Service (NHS) provides a clear rationale for the timely adoption of the NIS Directive. The issue with hacking medical records is far from new. It was already the subject of discussion in the UK back in 1991 when the 'unpleasant aspects of these new systems of technology' were acknowledged in relation to hacking into hospital computers.

Yet 26 years later, the WannaCry attack caused major disturbances and a halt to the work of the NHS. The virus hit devices using Windows XP – an outdated and unsupported version of Microsoft software, highly vulnerable to attacks, a fact the NHS was aware of.

However, even though the NHS is a critical infrastructure sector, there is currently no law in the UK that enforces security measures for network and information systems, which, if present, would have technically prevented the attack.

This gap was also acknowledged in written evidence provided by Google, Yahoo, Microsoft, Apple, Twitter and Facebook on the Investigatory Powers Bill, which argued that the draft bill failed to provide statutory provisions on 'the importance of network integrity and cyber security'. In cases like this, the great importance of the NIS Directive becomes obvious.

Even though the NIS Directive is an excellent initial step towards better coordination and safer cyberspace across the Union, it will be years before its effectiveness can be demonstrated. The problem is that the process of adopting law is time-consuming and cannot keep pace with technology. Laws cannot be amended immediately after a new network, device or software update has occurred. There are always going to be zero-day vulnerabilities to be exploited by security agencies and/or criminals. What the NIS Directive can do, however, is minimise the risk of further Wannacry incidents.

Author Information:
Eva Saeva
Newcastle University

Eva Saeva is PhD Candidate in Law at Newcastle University. Her research concentrates on the EU's legal approach to cybersecurity.

Additional Information:
Please note that this article represents the views of the author(s) and not those of the UACES Student Forum or UACES.