INTERNATIONAL REGULATIONS IN THE FIELD OF NETWORK SECURITY AND COMPUTER SYSTEMS. INCIDENTS IN CYBERSPACE

MSc. Edmond Fierza\(^1\)
Lezhe, Albania

Dr. Adrian Leka\(^2\)
University “Luigi Gurakuqi” Shkoder
Shkoder, Albania

Abstract - The complexity of managing cybercrime incidents has recently been addressed (at national and international level) by regulatory authorities and policy designers. In this paper, cyberspace will be considered as a domain addressed in security aspects, both for information security and cyber space protection, the latter focused on military methods and national security methods for cyber space security. Beyond the national security aspect, it also includes other background systems that deal with the causes and consequences of incidents in the cyber space, such as economic domains, those of classified information collection and those of policy. When these domains are deployed in the context of policy, these domains will be interconnected with various legal disciplines that include proactive measures and measures after incidents occurring in the cyber space, both nationally and internationally. To avoid the application of template methods or uniformity to incidents in the field of cyber space, it is critically important to formulate the framework of the arrangements, measures that deal with all the complexities related to the matter, but it also provides sufficient clarity to to allow the authorities charged by the law on the protection of nations and computer networks to undertake legitimate, well-coordinated and proactive actions or decisions.

Keywords- cyberspace, strategy, incident, cyber crime;

I. INTRODUCTION

Crime is a social and economic phenomenon and is old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment". Three inseparable axes of contemporary cyber space; of pyramid - a lawful response to security issues in cyberspace; and, of the screen - the digital environment, the environment in which the incident occurs and the interactions are carried out to resolve it.

II. LITERATURE REVIEW

The purpose of this literature review is to provide an overview of the most relevant, previous research done on the legal laws that focus in internet users, electronic discovery challenges, law responses to the problem to these security threats and large-scale data breaches and finally to evaluate the current limitations in laws and regulations.

III. CUBE: POSSIBLE, ALLOWED AND PREFERRED

It is said that politics is the art of the possible, but it would be more correct to say that today the word technology is the art of the potential, in pot the same way that law is the art of permissibility and politics is the art of the favorite. The cube concept is merely a name for the organization at the highest level to reflect these three dimensions. Conventionally displayed such a cube would have an X axis for technology (possibly); and for Y axis to have Politics (preferable). Each of these dimensions would have a rich detailed hierarchy with supportive information. The Axis, or the dimension of politics, for example, can be thought of in six categories: diplomatic, classified information, military, political, legal and economic, or as the term DIMPLE. The composition of DIMPLE could allow decision-makers (policy makers/implementers) for each application area to access the information content from a perspective to include as much accurate information as possible and how much with little information unrelated to the case, to be possible. Determining one's interests and the underlying situation (in fact) on the cube axles would be easy to assess, what if there are any, legal and political instruments exist, which a political planner, policy-maker needs to take into consideration when dealing with handling, responding to incidents of incidents in cyberspace, or attacks that impede access to or operation of services (DoS, DDoS) as part of their national cyberspace strategy. In addition, each space can be arranged with a permissible dictionary and a common (customary) structure to add detail to the bull, taking the cybernetic incident and the predicted responses to
the case, for example each may be able to narrow the doubt up to where data protection instruments and relevant policy-making developments address the possible filtering of network data.

It will be difficult to address/treat all the instruments and methods at every stage of the cube model. Based on the analysis of the relevant international instruments, the cube would show the gaps and inconsistencies of international law and policy in the field, and when it develops further as a concept at the national level, it can also serve as a tool or a policy tool for policy makers and lawmakers to support new country-based instruments and methods against cyber-crime threats as far as possible.

The technology dimension, the cube, will be based on cyber threat threat assessment and incident experiences. It can reflect the scientific way of thinking, like Cris Scott, at Lincoln Laboratory, at the Massachusetts Institute of Technology, Boston, USA. Scott raises from the technological point of view “attack components in the cyber space” to the attack vector (user space, car language level - kernel, and others); hostile objectives (cognitive, as if they were filtering, disinformation and denial of access); and classes, categories of cyber attack (introduction, byzantine and life cycle). Another way to look at the axis of the technology would be to look at the types of incidents in the cyber space related to cyber bullying for different countries and international organizations, pre-designed and protective measures (such as filtering) and related levels responses (eg measures that can be taken at the level of the level, organization, or governmental level, as well as the necessary international commitments).

The great complexity of the various options and the variety of possible schemes of organizations can be thought of for a META structure such as cube - Technology / Law / Politics.

- **PYRAMID**
  The pyramid is a conceptual framework that allows us to organize the security implementation process for the cyber space compared to the cybernetic security content (content).

  ![Fig.2 Pyramid](image)

  ![Fig.1 Illustrative figure](image)

Fundamental, Basic, Assumptions are black and white rules (Yes or No; actions or no actions) implemented in a random system - with options, logical decision making conditions: If or then (if or then) based on objective criteria and does not require repetitive interaction with the threat. Examples may include automatic disconnection from a server by receiving a code known as corrupt, or isolating a request from a user that comes from an hostile source(device or system). Assumptions should be made to be as close as possible, in the sense that they should be applied without further thought or authorization from any automated system. The benefit of such a scheme with assumptions is decision - making and response to the milestone fraction threat.

This can be considered as equivalent to the instruction provided by non-lethal guards to “snap” the neighbor who approaches the wire siege of their military base near the enemy territory and then proceed with the identification of the violator and the notification procedure, just after the neutralization of the threat to the cast has been made. To be law-abiding and prudent, such assumptions or manuals should be applicable against any potential threat to which they are supposed to behave. Perhaps the more concrete application for these assumptions, the manual procedure, would be the first legitimate and necessary defense line applied to SCADA systems, the compromise of which could threaten thousands of lives. Gradually, the assumptions may refer to the right (proper) expectations for cyber threat management, such as the appropriate quality and validity of the filing logs that must be applied by all companies providing Internet services.
Intermediate level, the algorithm is also realized by the automated system, but it includes a logical tree to authorize further protection actions. The request for additional information will condition a recurring process through which the system will quickly collect the required minimum required data to meet the “use of force” criterion in the cyber space, at the speed of cyber courses. These algorithms are simpler than the “yes or no” logical criteria, but even here it is possible to meet a sufficiently fast system to react to a devastating attack on time in order to avoid damages and serious consequences. To continue with our analogy with actions in the field of defense, this would be similar to the guard sergeant, who was instructed to observe and investigate possible violators, to warn them with a violation - knowing signal, before ordering the soldiers guards to open fire. Computer desktops and computer systems are capable of "instructing" to detect potentially harmful activities (disenchanting) and engage in additional controls on such signals.

The pyramid's highest peak - The law is most controversial and less consuming - less programmable in time. At this level, the human factor must become part of the decision-making process to make important decisions based on unclear or even contradictory information. There is a demand for the personal responsibility of the human factor as part of the process and that the person has the presence of a counsel from a legal consultation. In these cases the answer could be delayed by minutes, or mostly for a few hours. The benefit is in the quality of the final product; the cost is related to the delay in response that can move a cyber space from the immediate defense stage to a stage with sufficient scrutiny and planning and planning to look more like an attacker in nature. To conclude with our analogy with the real world, this would be in the hands of a basic commander that takes several hours to consult with law experts to calculate the range of possible responses to civilian protesters who threaten to break the perimeter of base security by placing both soldiers and their bases at risk. The wider effects of such a decision would require consultations with the highest levels of command hierarchy and with high probability would include a judgment, political decision to mitigate options or legal responses to the response.

To provide the answer to Pyramid's legal level, it is critical to carry out clear and accurate legal analysis. Measures to avoid or manage an incident in the cyberspace will need to be definitely supported in the final stage by definitions, legal definitions, but these legal provisions may not always be completely clear and easily understandable to the decision-maker. Furthermore, the analysis carried out by legal experts will have to take into account the needs of the concrete event provided by the provided information and by the authorities for the protection and management of the cyber space and results in conclusions that assist the experts in the matter or other aspects, to apply as models of responses to incidents that may occur in the future.

The pyramid can be constructed, conceived as well-modeled and overturned, in the sense that the analysis of existing legal instruments at the international level will orient the standards that will be most widely applicable to all jurisdictions. Where international instruments are not directly related to the event, Algorithms and Assumptions can be based on legal risk analysis, taking into account the best practices at the national level, as well as the best internationally accepted models for the management of cross-border incidents of cyberspace. However, it should be recalled that since Assumptions (hypotheses) are intended to act automatically and without the influence of the human factor, they should reflect undefined (unclear) decisions / actions in accordance with the law on protection against virtually any potential (potential) violator. The challenge will be to maximize possible options at all three levels, automating as far as possible the process according to the legal precondition, technological intelligence, as politically acceptable as possible, in practical terms.

- **SCREEN**

The screen is the final tool in this paper. Any theoretical constructs to fit and whatever they are put into practice should be placed in a form that is as simple and quick accessible to the specialist engaged in incident management in cyberspace. The term screen is simply a necessary term for the graphical user interface that will show the status and tendency, threats and options, propensity and gaps in the information. Although the perfect knowledge of all pertinent threats is an impossible goal, it is realistic to do even more to provide a clearer and more integrated overview of security in our cyber space for technology, advocates and policy makers who will have to collaborate to avoid the next attack that can be made on cyber systems.
One can think of the screen as a sophisticated user-orientated information system that supplies / distributes hundreds of databases in an interactive, simple way to access and use them. Its visible part would be an Internet space that would provide good structured information about the categories presented as cube shafts. It could contain educational material, learned experiences, concrete proposals, as well as appropriate legal and political instruments, providing expert and decision-making levels of instructing for various security aspects in the cyberspace.

The screen concept can also serve to identify people, organizations, and authorities that can contribute to the process of cybercrime management. As such, the screen would provide not only a model for decision makers but also speed up communication on incidents in the cyberspace between state governments and experts on specific issues.

IV. RECOMMENDATIONS FOR IMPLEMENTATION LEVELS OF DIFFERENT COUNTRIES

The application of the Directive is related to its field of application. In accordance with Article 3 (2) of the Data Protection Directive, it shall not apply to the processing of personal data under the conditions of an activity which is part of Community law and in any case to processing operations connected with public security, defense, state security (including the economic well-being of the state when the processing of data is related to State security issues) and the State's activities in the aspects of the implementation of the criminal law.

Similarly, Article 15 (1) of the e-Privates Directive defines the conditions under which EU Member States may limit the scope of the rights and obligations which are ensured in this Directive. Any such confinement should be necessary, appropriate and proportional to the aims of a public order in a democratic society, namely, to safeguard and ensure national security (ie the security of the state and its citizens) protection, public safety or prevention, investigation, detection and prosecution of criminal offenses or unauthorized use of electronic communication systems.

Another perspective that could potentially play a role in the debate over the application of the Directive on the processing of data traffic is to process information on network monitoring for law enforcement effects and for other additional purposes related to national security of electronic communication systems.

Nations, and different countries may use the exclusion for national security purposes provided for in the Data Protection Directive. The general exclusion of national security should also be included in other legal instruments, mainly related to the authorities and procedures that apply, or are included.

V. INCIDENTS IN THE CYBER SPACE, ESTONIAN CASE

- The stages and times of the attack

Cyber attacks began in parallel with violent road demonstrations in late 27 April, when Estonian Internet institutions and government websites and information portal portals underwent a wave of attacks on space cybersecurity. Estonian government's infrastructure and utilities were hit by a wave of cyber-space attacks with varying degrees of intensity by the end of May when tensions between Estonia and Russia over the bronze soldier's issue began to soften.

The first phase appeared on 27-29 April and was considered to have been emotionally motivated, as the attacks were relatively simple and if it was discarded, it appeared on mutual assistance grounds.

The first phase was followed by the main phase of the coordinated attack, which lasted from 30 April to 18 April, which was more sophisticated and used the world and where professional coordination was observed. Obviously, a clear correlation was observed between important political dates and the intensification of the attacks.

- Emotional Response (27-29 April)

The first attack on the internet sites of the river was reported to have appeared in the late hours of 27 April, 2007. Also in the early days were attacked also online media portals and news media portals that disseminated news about the demonstrations on the street and the general political scene.

Initially, attacks were carried out with relatively simple tools and were therefore figuratively named "Demonstrations in the Cyber Space". Various Internet forums in Russian were noticed calls and instructions to start ping commands (simple commands to check the validity of attacked attack
computers) with certain parameters in the command line MSwindows. Later appeared a file with executable command prompts with the .bat command that copied users would copy to their computers unencrypted files that would serve to launch authorized requests with the ping command.

This would result in attacks on denial of service for these computers, their release from work (DoS); although coordinated these attacks were effective in disrupting their objectives. The attacks were also coordinated through online chat forums (IRCs).

Phase with ping attacks was followed by malicious requests for websites that were mainly used against official government websites and media portals - this was already a more specific use of these tools as an attack tool. So this phase of the 27-29 April attack was simple, not coordinated to the right extent and was therefore easily resolved.

- **The main attack ( 30 April - 18 May)**

In the second phase, more sophisticated and coordinated attacks were introduced in four main waves, which we will describe below. Compared with the first stage which could be considered as emotional, the second stage was clearly characterized by its use in large amounts of botnets. As a top-level attachment co-ordination attachment as an initial method using internet forums for instructional deployment and attack target lists, they were used as the first stage. The instructions were generally simple without requiring a high level of technical knowledge or skill to accomplish; a computer with an internet connection was sufficient to be part of the attack.

Calls were made to plan attacks at specific time in order to generate a large, simultaneous request volume with a view to having as much impact on attack facilities as possible. Discussions on how to fund server leases and botnets and denial of server service attacks were also present.

Domain names (DNS) servers and routers that were the Elion company were repeatedly attacked from 30 April to 18 May, causing temporary disruption to services. In addition to the rainy days the attacks were at the maximum as described below, the traffic would continue to be at higher levels than usual throughout this period of time.

In most cases the attacks were manageable but some Internet addresses were worse off by the attack and remained inaccessible for certain time periods.

- **Ways and types of attacks on Estonia**

The attack tools used in the April-May 2007 events include blocking the service (DDoS) deleting content of Internet pages as well as large amounts of comments and spam. Public propaganda set up in many internet forums and the spread of attack instructions were used to promote, coordinate, and assist in conducting attacks.

- **Type Attacks (DoS) and Distribution Attacks (DdoS)**

In the early days of the cyber space incident to Estonia, most of the attacks were for denial of service (DoS) and the other DdoS attack, attacks that resulted in inaccessible access to the attacked Internet pages.

A DoS attack is a deliberate attempt to deny access to any electronic device, computer, server, network, or internet source to its users that require that service. Such a thing can be achieved in a number of ways: sending a giant amount of ping requests, sending massive UDP requests, and badly formulated questions were some of the tools used in the case of attacks in Estonia. Malicious GET issues, SYN type update requests, and the so-called death ping-death command were among the methods used.

The effect of DoS attacks was the worst extent of users outside Estonia, as a large amount of “question” requests were deliberately interrupted in order to deal with trafficking increased and allowed just traffic, as part of the permanent network operation. At the maximum time of the attacks, the amount of traffic from outside Estonia with sites and websites servers of government institutions was 400 times higher than normal traffic.

- **Attacks of DNS Servers**

An even more dangerous trend was the attack on DNS servers managed by Internet Service Providers. Repeated attacks on DNS servers and root managed by the company Elion were observed in the interval from 30 April to 18 May. Some of the attacks were successful in short periods of time, temporarily disrupting DNS service in parts of the country.
Attacks objective

The main objectives (and of course the ones most affected) were government and private sector information channels, as well as business websites, specifically banks.

The work of databases, systems or registers of the private and public sector was not interrupted, but there were attacks aimed at damaging the national Internet infrastructure. Also, the common emergency number 112 was the subject of the attack, so there were certain periods, short times when this number was unavailable, blocked.

The institutes’ servers in the state of Estonia for the Internet Infrastructure of the whole country. Governmental and political objectives, services provided by the private sector, individual and casual objectives.

VI. CONCLUSIONS

Concepts for Cube, Pyramid and Screen represent complementary methods to make clear the complexity of international conflicts in cyberspace. These tools include a system that is able to evolve quickly - perhaps at the international level. This version is possible to later become available for comments and processing at communitarian levels. With academic and operational contributions, evolution for the assessment of threats in the cyber space and the lessons we will face in the future, the system is possible to be improved and perfected, to include the range of complexity and different organization methods developed at national level. The conceptualization of three overlapping concepts represents the status of cybernetics and politics and emphasizes relevant issues for regulatory authorities and policy enforcement or policy enforcement at the international, national, and private level level. More advanced national models could provide valuable input into potential legal issues, in response to threats to incidents and the consequences they may bring. Over time, these instruments would help clarify the dark legal and policy issues of implementation, as well as the identification of impractical legal restrictions that need to be revised both at national and private level. Is demonstrated that regulation is necessary in the cyberworld in order to maintain and uphold rights in the real world as well as in the cyberworld. The form of the regulation should not be a purely legalistic one that simply transposes the existing real world laws. Nor should the regulation be in the form of socio-normative self-regulation. Instead, the best regulatory mix is that which combines the legal, with the socio-normative with considerations of the contextual. Contextual factors include the Internet architecture and utilises the Internet architecture to enhance the regulation provided by law and social-norms.

REFERENCES