REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

VOL. 7 NÚM. 2 (2018) • PÁGS. 5-25 • DOI 10.5354/0719-2584.2018.51028
RECIBIDO: 25/8/2018 • APROBADO: 12/11/2018 • PUBLICADO: 30/12/2018

DOCTRINA

Defining cyberterrorism

Una definición de ciberterrorismo

Laura Mayer Lux

Pontificia Universidad Católica de Valparaíso, Chile

ABSTRACT The aim of this article is to define cyberterrorism. With that in mind, the first part of this article analyzes the notion of terrorism, a broad category to which the species "cyberterrorism" belongs. The second part of this article is about determining the scope of the term cyberterrorism, and presenting the challenges that this creates in a global and technologically interconnected world.

KEYWORDS Terrorism, cybercrime, computer sabotage, critical infrastructures, terrorist.

RESUMEN El presente trabajo tiene por objeto definir el concepto de ciberterrorismo. Con dicha finalidad, la primera parte del artículo analiza la noción de terrorismo, género al que pertenece la especie «ciberterrorismo». La segunda parte del trabajo, en cambio, se dedica fundamentalmente a delimitar el término ciberterrorismo y a plantear los desafíos que éste supone en un mundo global y tecnológicamente interconectado.

PALABRAS CLAVE Terrorismo, cibercrimen, sabotaje informático, infraestructura crítica, terrorista.

Introduction and approach to the problem

The term "cyberterrorism" is complex and combines two concepts: "cyber", referring to cyberspace, and "terrorism", whose meaning and scope will be analyzed later. On this basis, we can assume that cyberterrorism is a special type of terrorism, where the "place" or "medium" it is carried out in is cyberspace (Conway, 2014; Denning, 2000). Cyberspace is considered "a globally interconnected network of digital information and communications infrastructures" (Melzer, 2011: 4), normally understood to mean the internet and, more broadly, computer networks (Ambos, 2015; Yannakogeorgos, 2014).

The concept of cyberterrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks. As such, in order to better understand what cyberterrorism is, this article will begin by analyzing the concept of "terrorism" –including its structure, harm principle, and elements– as a broad category to which the species "cyberterrorism" belongs; later, it will delimit the idea of cyberterrorism and distinguish it from others with which it has a certain similarity; finally, it will raise some of the most important challenges that cyberterrorism implies in a global and technologically interconnected world.

What is terrorism?

Much has been written about the concept of terrorism, but without agreement on its meaning. Many authors on this topic have pointed out the difficulties in forming a legal definition of terrorism, differentiating it from other types of crimes (Fletcher, 2006; Guzmán Dalbora, 2017). However, there is consensus that terrorism is not just regular crime, but constitutes a special form of crime, characterized by its severity (Teixeira, 2013). In that sense, "the better way to think of terrorism . . . is not as a crime but as a different dimension of crime, a higher, more dangerous version of crime, a kind of super-crime incorporating some of the characteristics of warfare" (Fletcher, 2006: 900).

In considering some of the main ideas developed in relation to the legal definition of terrorism in the Continental European framework, there is general agreement in how it relates to the structure, harm principle and elements of terrorism. The Continental European framework is relevant because of its extensive work on the theoretical-dogmatic concept of terrorism.

Structure

In terms of its structure, terrorism is always organized crime (Cancio Meliá, 2010), as opposed to individual crimes (for example, bodily harm caused by a single person) or crimes carried out by a group on an ad hoc basis (for example, a homicide committed by three individuals: one to subdue the victim, another to stab her in the abdomen, and a third waiting for them in a getaway car.)

In effect, although some authors believe terrorism can be carried out by a single person (Goodman, Kirk & Kirk, 2007), others claim, correctly, that (in practice) there is no such thing as "individual terrorists" acting alone, outside of an organization (Villegas Díaz, 2016). Thus, the specific "danger" implied by terrorism (Cancio Meliá, 2010), which in part justifies its severe punishment in relation to other crimes,

lies in the existence of an organized collective that operates systematically to commit an indefinite number of crimes (Gómez Martín, 2010). Regardless of the problematic nature of the concept of "danger", due to its great indeterminacy and incompatibility with the presumption of innocence, such danger does not exist in the case of an individual or ad hoc group acting alone, even if they employ similar methods (for example, explosives) commonly used by terrorist organizations. For the same reason, if a single person detonates a bomb on a public street there would certainly be some criminal conduct, but not a terrorist act based on the arguments outlined earlier.

In relation to these requirements, a doctrine has developed providing criteria to determine whether a "criminal terrorist association" is faced. They are: 1) the existence of a set number of members, 2) access to resources and funding, and 3) a capacity to sustainably plan and carry out operations over time (Mañalich, 2015).

Harm principle

Regarding the harm principle (Von Hirsch, 1996), terrorism does not directly attack individual interests (for example, life or property), interests that are owned or serve a specific person or a set group of people (Kindhäuser, 1989). On the contrary, terrorism immediately affects a collective interest (Asúa Batarrita, 2002), an interest that is owned by or serves the general public (Corcoy Bidasolo, 1999). In the case of terrorism, the collective interest directly attacked is identified with the democratic constitutional order, which is defined narrowly as "the constitutional guarantee of manifesting itself through the legal and material channels of democratic participation" (Villegas Díaz, 2016: 160). Hence, it is affirmed that terrorism constitutes an attack against institutional (Mañalich, 2017), state (Gillespie, 2016), or national (Jones, 2005) interests.

Said characteristics distinguish terrorism from common crimes like homicide or assault, which immediately affect individual but not collective interests. Even if terrorism harms or threatens individual interests like the life or health of others, this indirect impact is not its goal. Instead, the goal is a direct attack on the democratic constitutional order.

By linking the harm principle to the structure of terrorism, it can be concluded that keeping the democratic constitutional order in check requires more than the mere existence of a group of individuals: it requires a certain "organizational density", that is, a structure for collective decision making, to coordinate and persist over time (Mañalich, 2017).

Considering the harm principle described, a wide range of situations can be established, ranging from minor to severe.

First, that only the collective interest of "democratic constitutional order" is threatened. This can happen if an individual joins or is part of a terrorist organization

with a criminal agenda. In this case, for these interests to be at risk, indications that threatening actions against the democratic constitutional order have been taken are necessary (Villegas Díaz, 2016).

Second, that the collective interest of "democratic constitutional order" is violated, with one or more individual interests threatened. Such a situation may occur when propaganda is used to destabilize a political regime, in which, for example, the life or health of others is put at risk. In reality, those situations normally require certain technologies, with propaganda usually being spread via the internet. In addition, the threat in question should be plausible or credible (Denning, 2011), as terrorist groups utilizing propaganda to make laughable or absurd threats towards others should not be considered terrorism.

Third, that the collective interest of "democratic constitutional order" is violated as much as one or more individual interests. This can happen if a terrorist group, in order to execute a particular political agenda, takes control of a train and sets its course to collide with another, causing, for example, death or injury to its passengers.

Elements

In terms of the elements, terrorism is comprised of a teleological element and instrumental element.

Regarding the teleological element, terrorism must be committed "with the aim of altering the constitutional order or to topple the legitimately elected government" (Villegas Díaz, 2016: 161). By extension, terrorism, unlike other types of crimes, is always politically motivated (Weimann, 2005) and expresses a political message (Crenshaw, 1981; González Calleja, 2016). In other words, it is a radical form of political violence (Della Porta, 1995). Although demonstrating these facets of terrorism can be complicated in practice, it is possible to infer the presence of certain clues —among them, the remaining requirements of the notion of terrorism (structure, harm principle, and instrumental element.) Thus, it avoids falling into a "psychologization" of the concept of terrorism (Mañalich, 2015) which would likely be produced by defining terrorism exclusively or fundamentally based on the aims of those committing terrorist acts.

In terms of the instrumental element, terrorist acts must be executed in a manner appropriate to instill terror in people's minds (Villegas Díaz, 2016), establishing a belief that anyone anywhere could be a victim of terrorism (Carnevali, 2010).

Regarding the use of appropriate means to cause terror, some authors argue that buildings or crops could be the targets of terrorist attacks (Gibbs, 1989). However, these attacks must have flow-on effects that impact actual people. In other words, it is insufficient for terrorist acts to merely impact inanimate objects or private property. Rather, terrorists must direct their attacks to deliberately target civilians (Ganor,

2002; Mañalich, 2017). This can be achieved by directly attacking people or other targets (such as hospitals or schools) which result in deaths, serious injuries, or other similar outcomes. This conclusion is consistent with the idea, previously proposed, that the better way to think of terrorism is not as a crime but as a different dimension of crime, a higher, more dangerous version of crime, or a kind of super-crime incorporating some of the characteristics of warfare.

In terms of the relative uncertainty surrounding the specific objectives of terrorist attacks, as terrorism employs indiscriminate violence (Sorel, 2003), if a terrorist organization threatens to assassinate a specific political leader and carries out such threat to kill them, this would not constitute terrorism, as it lacks the very uncertainty mentioned earlier.

The existence of terrorism jointly requires the structure, harm principle, and both elements (teleological and instrumental) previously outlined. If one or more of these requirements is missing, then terrorism cannot be said to exist. It is the presence of these three requirements that differentiate terrorism from other acts, be they criminal, such as threats or "hate crime" (Boeckmann & Turpin-Petrosino, 2002); or be they non-criminal, such as membership of or activism by extremist political or religious groups. That said, it remains possible that membership of or activism by extremist political or religious groups may result in the carrying out of terrorist acts, but for this to happen it is necessary, as mentioned, for the above three requirements to be present.

What is cyberterrorism?

Much has also been written on the topic of cyberterrorism, despite lacking a unanimous consensus regarding its scope and meaning. As it were, for cyberterrorism to be, effectively, a form of terrorism, it must meet the structure, harm principle and elements of terrorism. As a result, the scope of cyberterrorism is, as its name suggests, based on the "place" in which it occurs or the "medium" through which it is carried out: in cyberspace instead of the physical world. From this point of view, cyberterrorism is not an autonomous crime, which should be punished independently. Rather, it implies a kind of terrorism characterized by a unique method of execution.

That cyberterrorism is defined by its location or the medium through which it is executed can be criticized to some extent. To address such criticisms, a comparison can be made to aircraft hijacking terrorist acts, such as the 9/11 terrorist attacks on the World Trade Center; or vehicle-based terrorist attacks, such as when a truck deliberately drove into a crowd of people on the Nice promenade in 2016. In reality, the scope of cyberterrorism appears to follow the general tendency for many "real world" phenomena to be replicated online. Thus, it is common to talk about "cyber activism" (Milan & Hintz, 2013) as a type of activism carried out online; or "cyberbullying"

(Kraft & Wang, 2009) being a type of bullying which also occurs online. Similarly, it's not difficult to imagine that, with the rise of terrorism, there has also emerged it's virtual strain: cyberterrorism.

The (cyber)terrorists' actions and the (cyber)terrorists' author

The Continental European tradition of criminal law usually differentiates between what an individual does (in other words, their behavior) and who they are (in other words, their character, personal preferences, thoughts, etc.) From this, we can distinguish between the criminal law of "acts" or "facts" (Mir Puig, 2016), consistent with a liberal criminal justice system, and the criminal law of "author" (Velásquez Velásquez, 2009), consistent with an authoritarian criminal justice system. The criminal law of "acts" is based on actions, such as theft or sexual abuse of a minor. The criminal law of "author" is based on dangerous criminal personality traits, such as if an individual is a thief or pedophile. At its core, under the criminal law of "author", a thief or pedophile is marked by a kind of stigma, wherein independent of their actions, and even though their theft or sexual abuse of minors is now in the past, they will forever be considered a thief or pedophile. This is linked to the concept of criminal law of "the enemy" (Jakobs, 2003), which treats those breaching the rules as enemies of the state rather than citizens "who are simply a source of danger that must be eliminated by any means, whatever the cost" (Cancio Meliá, 2002: 20).

That same form of discussion and analysis is often seen when discussing terrorism, where a (political) opponent is, strategically, labelled a "terrorist" (Mañalich, 2017). In such an approach, commonly seen as authoritarian or anti-liberal, the focus is on the "terrorist." Meanwhile, a liberal approach focuses on the actions of the so called terrorist more than their personal characteristics as a "terrorist."

The final approach to responding to terrorism is the correct one because, amongst other things, not all actions of a "terrorist" or by a member of a terrorist organization can be classified as terrorism or terrorist acts. In reality, a "terrorist" is far more likely to engage in a wide variety of activities ranging from non-criminal (such as spending time with family or driving a car), to committing non-terrorist crimes (such as fraud or drug trafficking), than to actual terrorist attacks (such as bombing the seat of government.)

The same applies to cyberterrorism. That is, an authoritarian or anti-liberal criminal law would focus on the "cyberterrorist", whereas a liberal criminal law would focus on the actions of the so called cyberterrorist more than their personal characteristics as a "cyberterrorist." Just like a "terrorist", a "cyberterrorist" can also engage in a wide range of activities online, ranging from non-criminal, to criminal but not terrorist, through to terrorist in nature.

However, it is possible to distinguish between two kinds of "cyberterrorist":

The first kind, likely to be more common, is the traditional "terrorist" that uses the internet as well as information and communication technologies to perpetrate their attacks. In this case, those carrying out traditional terrorist attacks take advantage of the benefits offered by these technological tools, for example the ability to negatively impact a large number of people in a brief period of time without personally physically exposing oneself (Weimann, 2005), but from the comfort of their own computer. This applies both in the preparation of crime (planning, conspiracy, etc.) and to their partial execution (attempted crime) or completion (successful crime.) In the case of attacks that make some use of technology, a terrorist can, amongst other things, attack the networks that allow for control and supervision of industrial processes, systems known as SCADA (Supervisory Control And Data Acquisition) (Poveda Criado & Torrente Barredo, 2016); or, damage "critical infrastructure" (Gercke & Brunst, 2009; Von Bubnoff, 2003), for example the water supply and potable water, means of transport and telecommunications, health services, etc., which in turn affect a considerable number of people.

The second kind is the subject falling within the "hacker" archetype who begins executing actions of escalating intensity: first by destroying data of actual users; then sabotaging information stored by a (large) company or (large) government entity; finally directing an attack against a SCADA or critical infrastructure through the use of technology. In this final case, we exit the scope of mere hacking and enter into cyberterrorism, as long as all the requirements (structure, harm principle, elements) are present which comprise actual terrorism. Assuming that there is a debate along the lines of what exactly is implied by hacking (Madarie, 2017), its definition can be derived from cyberterrorism's through exclusion. That is to say, it would be cyberterrorism if actions are executed "on" or "through the medium of" cyberspace and the required structure, harm principle and elements that characterize terrorism are present. If those requirements do not exist in practice, it may be a case of hacking or hacktivism (Hampson, 2012). For this reason, it can be said that cyberterrorism is always one step beyond mere hacking or hacktivism (Gillespie, 2016).

Notwithstanding this, it is possible to imagine links between hackers and organized crime, particularly terrorism. Beyond the situations where terrorists count hackers within its ranks –in which case it can be difficult to differentiate between (cyber)terrorism and hacking–, it remains possible for hackers to be motivated by profit and to contact terrorist groups in order to sell their computer skills or software that could be used in terrorist attacks (Wilson, 2003). Or, that members of a terrorist group turn to hackers whenever they seek to use cyberspace or technologies to commit an attack that they are not in a position to carry out themselves because they lack the necessary skills. As has been outlined in relation to terrorism (Mañalich, 2017), in these cases it should be possible to distinguish between the role played by the members of the terrorist organizations –"from within"– and that played by their

supporters (in this case hackers) –"from outside"– whose relevance in the criminal justice system depends on the impact they have on the existence and operations of the organization.

(Cyber)criminality and (cyber)terrorism

In the same way that any crime should not be confused with a terrorist attack (Poveda Criado & Torrente Barredo, 2016), the concept of cybercrime should not be confused with that of cyberterrorism (Weimann, 2005). In that sense and as already indicated, just as terrorism is always more severe than other forms of criminality, cyberterrorism is always more severe than other behaviors that are carried out "in" or "through" cyberspace. This approach seeks to avoid a "trivialization" of the concept of terrorism (Mañalich, 2015) and cyberterrorism, which would certainly occur if they were defined without considering the particular severity that characterizes both phenomena.

In order to better understand what has been pointed out, we must take into account not only the concepts of terrorism and cyberterrorism, in the aforementioned sense, but also the notions of computer crime, cybercrime, and common crime. It should be noted that although not all authors distinguish between computer crime and cybercrime, differentiating between them can be useful for analytical purposes.

Computer crimes can be classified into computer crimes in a broad sense and computer crimes in a strict sense. Computer crimes in a broad sense (Lara, Martínez & Viollier, 2014) are traditional crimes that are committed through computer mechanisms or the internet. Respectively, information and communication technologies have expanded the contexts or means of execution of certain traditional crimes, such as fraud (Gercke & Brunst, 2009) or sexual abuse (Clough, 2010), which can now also be committed through computers or the internet. Consequently, computer crime in a broad sense has also been called crime committed "through" computer systems (Marberth-Kubicki, 2010).

Computer crimes in a strict sense (D'Aiuto & Levita, 2012), on the other hand, are new crimes committed towards computer systems or the internet. Generally, these are actions that are directed against software. For this reason, this phenomenon has also been labeled as crime committed "against" computer systems (Marberth-Kubicki, 2010). This usually includes crimes such as computer sabotage (destruction or disablement of data or software), computer espionage (unlawful access or obtaining of data or software) and computer fraud (alteration or manipulation of data or software) (Jijena, 2008).

Cybercrimes are computer crimes (in a broad or strict sense) that are committed through the internet (Cárdenas Aravena, 2008; Clough, 2010). Unlike computer crimes, which are perpetrated "through" or "against" computer systems, cybercrimes are always carried out in a specific context: cyberspace. In this sense, what defines

a cybercrime is not its commission through or against a computer system, but a specific "place" or "medium" of perpetration. The categories "computer crime" and "cybercrime" are not mutually exclusive and can be present together. Therefore, the diffusion of child pornography through the internet constitutes a cybercrime and a computer crime in a broad sense, whereas the destruction of data from computer systems carried out in cyberspace constitutes a cybercrime and a computer crime in a strict sense.

Finally, common crimes are all those that cannot be classified as computer crimes or cybercrimes, or in any other way in particular. Thus, their definition is always determined by process of elimination. For example, theft is a common crime, in the same way that homicide is. If those crimes are committed by means of a drone operated by radio control, they do not classify as cybercrimes. The radio control is a closed system and so it lies outside of the internet. Although both examples can be committed using technology, they escape the phenomenon of computing or execution in cyberspace.

A subject that belongs to a terrorist organization can carry out all the activities discussed above, that is, computer crimes (in a broad or strict sense), cybercrimes or common crimes. In order to be classified as terrorist behavior however, the structure, harm principle and elements of terrorism need to be present. For cyberterrorism, moreover, terrorist behavior must be carried out "in" or "through" cyberspace.

Consequently, not all computer crimes (in a broad or strict sense) committed by a "terrorist" constitute terrorism or cyberterrorism. Not all the cybercrimes executed by someone belonging to a terrorist organization is to be described as terrorism or cyberterrorism. And, certainly, not all common crimes carried out by a "terrorist" are meant to be thought of as terrorism or cyberterrorism.

Neither is cyberterrorism configured when someone who belongs to a terrorist organization commits a terrorist act using technologies other than computer networks. For example, an organization that puts a bomb in a hospital full of patients where the trigger is a mobile phone activated through a telephone call. If that organization carries out such an attack in order to destabilize the democratic constitutional order, its behavior may be described as terrorism, but not cyberterrorism, since it was not executed in cyberspace or using computer networks.

The real cyberterrorism

So far, some problems have been described by the use of the term "cyberterrorism", as well as certain criminal behaviors that do not constitute cyberterrorism. Subsequently, some of the assumptions that correspond to cyberterrorism actions will be described, in order to specify the definition of this concept.

As previously insisted, for cyberterrorism to exist, terrorist behavior must be per-

petrated in cyberspace. And for terrorist activities to be executed in cyberspace, it is necessary that the behavior carried out "in" or "through" cyberspace has a structure, a harm principle and the elements that allow it to be classified as such. And all those requirements (structure, harm principle and elements) must be jointly present, otherwise, the conduct in question cannot be considered as cyberterrorism.

Structure

In terms of its structure, cyberterrorism is always organized crime, as opposed to individual (cyber)crimes (for example, a computer espionage committed by a single person) or (cyber)crimes carried out by a group on an ad hoc basis (for example, a computer sabotage committed by three individuals: one that develops malware, another that accesses a database and a third that uses malware to destroy certain data.)

In effect, although some authors believe in terrorism carried out by a single person and, thus, could also accept individual cyberterrorism, the specific "danger" implied by cyberterrorism, which in part justifies its high punishment in relation to other (cyber)crimes, lies in the existence of an organized collective that operates systematically to commit an indefinite number of crimes. Such danger does not exist in the case of an individual or ad hoc group acting alone, even if they employ similar methods (for example, destruction of critical infrastructure through computer networks) commonly used by cyberterrorist organizations. For the same reason, if a single person gains access to a computer network and modifies the information that is issued and received at the monitoring station of an airport, thereby putting the life or health of people flying on the monitored aircraft at risk, there would certainly be some criminal conduct, but not a cyberterrorist act based on the arguments outlined earlier.

In this context, to speak of a "criminal cyberterrorist association", there would have to exist, as with terrorism, a set number of members, access to resources and funding, and a capacity to sustainably plan and carry out operations over time.

Unlike in the case of traditional terrorism, the perpetration of terrorist and cyberterrorist attacks through the use of technologies could relativize the requirement that there be an organized collective composed of a certain number of "people." In fact, it is currently possible for a single person to comprise a botnet, that is, a series of computers called bots or zombies previously captured by that person. This capture is done through botware (Kochheim, 2015), malware designed to build botnets, which allows access and remote control of the various computer systems that make up the botnet (Choo, 2007). Due to this, it would be possible for a single controller of several bots or zombies to systematically commit an indefinite number of crimes.

However, that single person will never have the "organizational density" that is characteristic of terrorism, which implies the existence of a structure (of people) for collective decision making, to coordinate and persist over time. In this sense,

although the possibility of action by that single person to harm other people is amplified due to a botnet, they are not comparable with those of a real (cyber)terrorist organization, the only structure really capable of keeping those interests protected by (cyber)terrorism in check. The amplification of damages through the use of technologies can be observed in many cybercrimes, but that in itself does not justify classifying the behavior individual subjects as terrorist attacks.

Harm principle

Regarding the harm principle, cyberterrorism does not directly attack individual interests, that is, those that belong to or serve a specific person or a set group of people. On the contrary, cyberterrorism directly affects a collective interest, an interest that is owned by or serves the general public. As in terrorism, the collective interest directly attacked by cyberterrorism is the democratic constitutional order. Hence, it can be affirmed that cyberterrorism constitutes an attack against institutional, state, or national interests.

Said characteristics distinguish cyberterrorism from common crimes like homicide or assault, but also distinguish cyberterrorism from cybercrimes such as computer fraud, all of which directly affect individual rather than collective interests. In other words, even if cyberterrorism harms or threatens individual interests like the life or health of others, this indirect impact is not its ultimate goal, instead the goal is a direct attack on the democratic constitutional order.

Considering the harm principle described, a wide range of situations can be established, ranging from minor to severe.

First, that only the collective interest of "democratic constitutional order" is threatened. This can happen if an individual joins or forms part of a cyberterrorist organization with a criminal agenda. In this case, for these interests to be at risk, indications that threatening actions against the democratic constitutional order have been taken are necessary.

Second, that the collective interest of "democratic constitutional order" is violated and additionally one or more individual interests are threatened. Such a situation may occur when propaganda is used in cyberspace to destabilize a political regime, in which, for example, the life or health of others is put at risk. As was said with respect to terrorism, the threat in question should be plausible or credible, as cyberterrorist groups utilizing propaganda in cyberspace to make laughable or absurd threats towards others should not be considered cyberterrorism.

Third, that the collective interest of "democratic constitutional order" is violated as much as one or more individual interests. This can happen if a cyberterrorist group, in order to execute a set political agenda, remotely takes control, through a computer network, of a traffic light located on a railway line, and causes two trains

in the opposite direction to share the same route, producing, for example, death or injury to its passengers.

Elements

In terms of its elements, cyberterrorism is comprised of a teleological element and instrumental element.

Regarding the teleological element, cyberterrorism should be committed with the aim of altering the constitutional order or to topple the legitimately elected government. By extension, the cyberterrorist group will always have a political agenda (Warren, 2008). However, although demonstrating these facets of cyberterrorism can be complicated in practice, it is possible to infer the presence of certain clues, among them, the remaining requirements of the notion of cyberterrorism (structure, harm principle and instrumental element.) Thus, it avoids falling into a "psychologization" of the concept of cyberterrorism which would likely be produced by defining cyberterrorism exclusively or fundamentally based on the aims of those committing (cyber)terrorist acts.

In terms of the instrumental element, cyberterrorist acts must be executed in a manner appropriate to instill terror in people's minds (Denning, 2000), establishing a belief that anyone anywhere could be a victim of cyberterrorism.

As can be seen, the presence of the instrumental element is very complex in the case of cyberterrorism. In that sense, if one thinks of a terrorist attack perpetrated in the "real world", it becomes relatively easy to form the belief that anyone anywhere could be a victim of an attack. Thus, for example, if a terrorist organization carries out an explosive attack in a beach resort with tourists, it is expected that survivors will feel terror and imagine that they –or anyone who visits it– may be the next ones attacked.

Faced with the above, the question arises: When is a cyberattack capable of generating terror in people's minds? This question has an empirical and a theoretical answer. The empirical answer exceeds the aims of this article. The theoretical answer, on the other hand, must be present considering the kind of interests that are violated or threatened with the cyberterrorist act, beyond the attack on the collective interest of "democratic constitutional order."

To cause terror in people's minds cyberterrorism must involve the realization of an indiscriminate attack "in" or "through" the cyberspace, with consequences in the outside world that are identified with deaths, serious injuries or other similar outcomes.

Regarding the effects of the attack, it is insufficient for cyberterrorist attacks to merely impact inanimate objects or private property if it does not imply harm or at least danger to other interests, mainly the life or health of people.

Therefore, cyberterrorism is not just the manipulation of data or software that causes a large number of people to lose considerable sums of money through the internet, unless such loss entails economic ruin and a consequent impact on the life or health of its victims. The destruction of data that generates the loss of relevant scientific or academic information is also not a case of cyberterrorism, unless it implies danger to the life or health of others, for example, if the formula of a medicine is changed through the internet to make it harmful or even lethal (Hua & Bapna, 2013). Meanwhile, the mere attack of web pages by a cyberterrorist group, for example, DoS (Denial of Services) or DDoS (Distributed Denial of Services) attacks against sites supposedly contrary to the values of Islam (Denning, 2011) or belonging to state agencies (Hardy & Williams, 2014) do not constitute cyberterrorism. All these cases may involve the perpetration of computer crimes, cybercrimes or common crimes, but not cyberterrorism.

In terms of the means of the attack and, especially, the indiscriminate use of violence, cyberterrorism cannot target objectives that have already been publicly identified. For the same reason, if a (cyber)terrorist organization threatens to assassinate a specific political leader and carries out such threat to kill them using computer networks, this would not constitute (cyber)terrorism as it lacks the very uncertainty previously outlined. A case such as the one mentioned may involve the perpetration of a computer crime, cybercrime or common crime, but not cyberterrorism.

Instead, attacks against critical infrastructure using computer networks can constitute cyberterrorism (Denning, 2011; Lewis, 2002), insofar as it endangers actual people. Thus, for example, if a (cyber)terrorist group, through a computer network, modifies the information that is issued and received at the monitoring station of a port and thereby puts the life or health of people traveling on the monitored boats at risk, there would be cyberterrorism, so long as all the requirements of (cyber)terrorism already outlined (structure, harm principle, elements) are present.

In relation to critical infrastructure, perhaps one of the most spectacular cases on record was the 2010 attack on Iranian nuclear infrastructure through the malware "Stuxnet" (Meier, 2015). Its diffusion would have operated by means of an infected USB stick (Kochheim, 2015) that, when inserted into a computer connected to the network, would have entered the computer system and focused on the software that controlled the uranium centrifuge machines. While in principle this kind of attack can be described as cyberterrorism, some doubts arise regarding the accreditation of the teleological element that must be present in any (cyber)terrorist attack, since to date there is no certainty of knowing who would have perpetrated this attack and, therefore, what would have been their purpose or motivation to commit it.

The challenges that cyberterrorism creates

Like terrorism, cyberterrorism involves a series of complex challenges in a global and technologically interconnected world, especially for those who seek to prevent and repress its perpetration. Despite this, unlike terrorism, these are challenges that are more forward looking. So far, terrorist groups "still prefer bombs to bytes" (Denning, 2011: 3). In that sense, although cybernetic attacks can be cheaper (Weimann, 2005) and easier to execute than a physical attack (Jones, 2005), they are less dramatic and effective than attacks carried out in the "real world" (Lewis, 2002). However, cyberterrorism constitutes a threat against which certain precautions must be taken, especially if it is considered that it can operate as a complement or suitable support for traditional terrorism (Denning, 2000). From this point of view, it is very likely that terrorism tends to combine attacks in the real world and attacks "in" or "through" the virtual world (Hua & Bapna, 2013).

Because a terrorist group can use cyberspace for various purposes (Ariely, 2014), it is necessary to clearly distinguish between two situations. First, it is possible that a terrorist attack is carried out through cyberspace, which constitutes, given its structure, harm principle, and elements, a genuine case of cyberterrorism. Second, it is possible for a terrorist group to use information and communication technologies and, particularly, the internet to carry out a series of actions linked to the objectives it pursues. Such use of the internet will not necessarily constitute cyberterrorism but may lead to the existence of preparatory acts or facilitation of future (cyber)terrorist behaviors.

The benefits that the internet implies in this area are fundamentally related to the favorable conditions it offers for the elaboration of different plans and the execution of diverse behaviors (Cohen, 2002; Poveda Criado & Torrente Barredo, 2016). First, the increasingly reduced costs of connection to the network (Meier, 2015; Neubacher, 2014) allows anyone to access the internet at any time. Second, thanks to the relatively lower costs of state-of-the-art technologies, many subjects can profit from them, including for the commission of illicit actions (Grabosky, 2009) and, certainly, (cyber) terrorist attacks (Denning, 2000).

Linked to the above, the internet is a breeding ground to coordinate (cyber)terrorist attacks (Berner, 2003; Cohen, 2002). In that sense, this network allows communication between several people without requiring that they meet physically in the same place (Poveda Criado & Torrente Barredo, 2016), since it is always possible to connect remotely (Hua & Bapna, 2013). The members of a (cyber)terrorist group can resort to communication systems that use instant messaging mobile phone applications to exchange information. They can also use software for sending text, voice, and video messages (Gillespie, 2016) or even console videogame chats (Podhradsky, D'Ovidio & Casey, 2012), which lets its users, while playing, to communicate with

each other. The internet also allows for planning and implementation of an attack to be preceded by valuable information, since (cyber)terrorist organizations can use the network as a tool for surveillance and espionage of potential targets and victims (Gillespie, 2016; Wilson, 2003).

The internet provides favorable conditions for recruiting new followers (Cano Paños, 2008; Miró Llinares, 2012), from different causes. Moreover, since it is an area in which there is no direct contact between its various actors (Gordon & Ford, 2002), it is possible that not only subjects with a strong personality or character would be interested in being part of a (cyber)terrorist group, but also timid or introverted individuals and even people with psychiatric problems. From this point of view, cyberspace is a place that allows the incorporation and participation by everyone in all kinds of initiatives, including criminal or actual (cyber)terrorist groups.

In addition, cyberspace is an ideal environment to indoctrinate and train the different members of a (cyber)terrorist organization (Miró Llinares, 2012; Poveda Criado & Torrente Barredo, 2016). In that sense, it is possible that the members of the (cyber)terrorist group exchange ideas (or ideologies) and strategies of action, including technical knowledge (for example, the manufacture of an explosive or the development of software) to carry out attacks in the future. Moreover, cyberspace facilitates alliances between people and groups with similar objectives and interests, also allowing them to mutually empower each other (Gordon & Ford, 2002) in the sphere of (cyber)terrorism.

In cyberspace, it is possible to spread propaganda (Cohen, 2002) easily and automatically. The technical costs to transmit a certain message, while maintaining the anonymity of its sender (Weimann, 2005), are quite low and the communication in question can be disseminated and replicated without prior censorship, innumerable times and at full speed (Poveda Criado & Torrente Barredo, 2016). This allows for many people to know the message of a (cyber)terrorist group, even people who are not direct recipients of that kind of communication. With this, the (cyber)terrorist organization gains publicity (Goodman, Kirk & Kirk, 2007), notoriety, and eventual new sympathizers. In the same way, the internet allows a (cyber)terrorist group to announce the future execution of a (cyber)terrorist attack or to claim responsibility for and, if necessary, justify the previous execution of a (cyber)terrorist attack (Poveda Criado & Torrente Barredo, 2016).

Likewise, and this is particularly important, the internet provides adequate conditions to articulate financing strategies for (cyber)terrorist groups (Cohen, 2002; Gillespie, 2016). Financing mechanisms linked to cyberspace can be distinguished into two situations. In the first situation, members of a (cyber)terrorist group may commit cybercrimes to finance their various activities, for example, cyberspace fraud (Lewis, 2002). In the second situation, bank transfers may be made for sums of money (Goodman, Kirk & Kirk, 2007) obtained lawfully or unlawfully, while payments

may be made for the sale of goods or services online (Poveda Criado & Torrente Barredo, 2016). In any case, such sources of financing can be used to financially maintain the members of the (cyber)terrorist group, to recruit and train new members, and to prepare and execute attacks, amongst other things.

In the future, there are many areas that could become possible targets of cyberterrorist attacks. Consider, for example, the development of intelligent vehicles, whose driving could be controlled (Denning, 2011) by groups of (cyber)terrorists through computer networks; or the possibility that such organizations intervene, through the internet, in the navigation of ships and aircraft. To this can be added the remote alteration of sensitive databases, for example, those that establish the pharmaceutical industry's medication formulas (Weimann, 2005). The same can be said of a possible increase, even at a mass scale, in attacks against critical infrastructure. In this context, the more devices and infrastructure (linked to the life and health of people) depend on the existence and operation of computer networks, the more vulnerable these devices and infrastructure will be in the face of possible (cyber)terrorist attacks (Lewis, 2002). And the more likely that (cyber)terrorist groups will effectively exploit such vulnerabilities.

However, perhaps one of the biggest challenges involved in cyberterrorism has to do with the lack of certainty about its real dimensions and potential. In that sense, it is not clear to what extent the threat of cyberterrorism is exaggerated, even for economic reasons. Think, for example, of the complex industry that has in fact developed around cybersecurity, including conducting research and publishing documents, hiring experts, creating software, etc. (Weimann, 2005). Therefore, it is crucial that there is reliable information on the specific scope of the phenomenon of cyberterrorism, so that the various reactions that it generates are rational, proportionate and adequate.

Conclusions

Cyberterrorism is distinguished from terrorism by the "place" in which it is perpetrated or by the "medium" through which it is perpetrated, that is, cyberspace. From this point of view, cyberterrorism is not an autonomous crime, but implies a kind of terrorism characterized by a unique method of execution.

Cyberterrorism must comply with the structure, harm principle and elements that define terrorism. Consequently, if these are not verified, we may be in the presence of a cybercrime and not cyberterrorism (for example a computer sabotage.) In terms of its structure, cyberterrorism requires the existence of an organization destined to perpetrate (cyber)terrorist attacks. Regarding its harm principle, cyberterrorism must directly violate a collective interest identified with the democratic constitutional order. In terms of its elements, cyberterrorism must be executed with the specific purpose of altering constitutional order or to topple the legitimately elected govern-

ment; and must be carried out in a manner appropriate to instill terror in people's minds, establishing a belief that anyone anywhere could be a victim of an attack.

Finally, cyberterrorism creates several challenges in a global and technologically interconnected world. Committing cyberterrorism involves the use of the internet, which offers a series of advantages for those participating in the act. In addition, because the real dimensions and potential of cyberterrorism are not yet clear, reacting with preparation becomes difficult.

Acknowledgments

This article was written under the framework of Project Fondecyt 1161066: "Los delitos informáticos en el ordenamiento jurídico chileno: Análisis dogmático y crítico, y propuestas de lege ferenda" ("Cybercrime in the Chilean legal system: Dogmatic and critical analysis, lege ferenda's proposals.")

I thank Professor Myrna Villegas Díaz for her valuable suggestions in the preparation of this article.

References

Ambos, Kai (2015). "Responsabilidad penal internacional en el ciberespacio." *InDret*, 2: 1-32. Available at https://bit.ly/2QNF1D5.

Ariely, Gil (2014). "Adaptive Responses to Cyberterrorism." In Thomas M. Chen, Lee Jarvis & Stuart Macdonald (editors), *Cyberterrorism,* 175-195. New York: Springer. DOI: 10.1007/978-1-4939-0962-9_10.

Asúa Batarrita, Adela (2002). "Concepto jurídico de terrorismo y elementos subjetivos de finalidad: Fines políticos últimos y fines de terror instrumental." In Juan Ignacio Echano Basaldua (coordinator), *Estudios jurídicos en memoria de José María Lidón.* Bilbao: Universidad de Deusto.

Berner, Sam (2003). "Cyber-Terrorism: Reality or Paranoia?" *South African Journal of Information Management*, 5 (1): 1-4. DOI: 10.4102/sajim.v5i1.208.

Boeckmann, Robert & Carolyn Turpin-Petrosino (2002). "Understanding the Harm of Hate Crime." *Journal of Social Issues*, 58 (2): 207-225. DOI: 10.1111/1540-4560.00257.

Cancio Meliá, Manuel (2002). "'Derecho penal' del enemigo y delitos de terrorismo: Algunas consideraciones sobre la regulación de las infracciones en materia de terrorismo en el Código penal español después de la LO 7/2000." *Jueces para la democracia*, 44: 19-26. Available at http://bit.ly/2EpZzvI.

—. (2010). "El delito de pertenencia a una organización terrorista en el código penal español." *Revista de Estudios de la Justicia*, 12: 147-164. DOI: 10.5354/0718-4735.2011.15233.

Cano Paños, Miguel Ángel (2008). "Internet y terrorismo islamista: Aspectos criminológicos y legales." *Eguzkilore*, 22: 67-88. Available at https://addi.ehu.es/handle/10810/24994.

Cárdenas Aravena, Claudia (2008). "El lugar de comisión de los denominados ciberdelitos." *Política Criminal*, 6: 1-14. Available at https://bit.ly/2RSKlSM.

Carnevali, Raúl (2010). "El derecho penal frente al terrorismo: Hacia un modelo punitivo particular y sobre el tratamiento de la tortura." *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 35: 109-145. DOI: 10.4067/S0718-68512010000200004.

Choo, Kim-Kwang (2007). "Zombies and botnets." *Trends & Issues in Crime and Criminal Justice*, 333: 1-6. Available at http://bit.ly/2Eqrwna.

Clough, Jonathan (2010). *Principles of Cybercrime*. New York: Cambridge University Press.

Cohen, Fred (2002). "Terrorism and Cyberspace." *Network Security*, 5: 17-19. DOI: 10.1016/S1353-4858(02)05015-8.

Conway, Maura (2014). "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism." In Thomas M. Chen, Lee Jarvis & Stuart Macdonald (editors), *Cyberterrorism*, 103-121. New York: Springer. DOI: 10.1007/978-1-4939-0962-9_6.

Corcoy Bidasolo, Mirentxu (1999). *Delitos de peligro y protección de bienes jurídico-penales supraindividuales*. Valencia: Tirant Lo blanch.

Crenshaw, Martha (1981). "The Causes of Terrorism." *Comparative Politics*, 13 (4), 379-399. DOI: 10.2307/421717.

D'Aiuto, Gianluca & Luigi Levita (2012). *I reati informatici*. Milan: Giuffrè.

Della Porta, Donatella (1995). *Social movements, political violence, and the state: A comparative analysis of Italy and Germany*. Cambridge: Cambridge University Press.

Denning, Dorothy E. (2000). "Cyberterrorism." Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Available at http://bit.ly/2Er9ZLt.

—. (2011). "Whither Cyber Terror?" In *10 Years After September 11, A Social Science Research Council Essay Forum*. Available at http://bit.ly/2EsnYkn.

Fletcher, George P. (2006). "The Indefinable Concept of Terrorism." *Journal of International Criminal Justice,* 4 (5): 894-911. DOI: 10.1093/jicj/mql060.

Ganor, Boaz (2002). "Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter?" *Police Practice and Research*, 3 (4): 287-304. DOI: 10.1080/1561426022000032060.

Gercke, Marco & Phillip W. Brunst (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: Kohlhammer.

Gibbs, Jack P. (1989). "Conceptualization of Terrorism." *American Sociological Review,* 54 (3): 329-340. DOI: 10.2307/2095609.

Gillespie, Alisdair (2016). *Cybercrime: Key Issues and Debates*. London, New York: Routledge.

Gómez Martín, Víctor (2010). "Notas para un concepto funcional de terrorismo." In José Ramón Serrano-Piedecasas Fernández & Eduardo Demetrio Crespo (coordinators), *Terrorismo y Estado de derecho*, 25-52. Madrid: Iustel.

González Calleja, Eduardo (2016). "Los estudios sobre terrorismo: Balance de los últimos 25 años." *Espacio Abierto, Cuaderno Venezolano de Sociología*, 25 (4): 61-76. Available at http://bit.ly/2ErZnvH.

Goodman, Seymour E., Jessica C. Kirk & Megan H. Kirk (2007). "Cyberspace as a medium for terrorists." *Technological Forecasting & Social Change*, 74 (2): 193-210. DOI: 10.1016/j.techfore.2006.07.007.

Gordon, Sarah & Richard Ford (2002). "Cyberterrorism?" *Computers & Security*, 21 (7): 636-647. DOI: 10.1016/S0167-4048(02)01116-1.

Grabosky, Peter (2009). "High Tech Crime: Information and Communication Related Crime." In Hans Joachim Schneider (editor), *Internationales Handbuch der Kriminologie*, 73-101. Berlin: De Gruyter.

Guzmán Dalbora, José Luis (2017). "El terrorismo como delito común." In *Colectánea criminal: Estampas de la parte especial del derecho penal*, 203-255. Montevideo: B de F.

Hampson, Noah (2012). "Hacktivism: A New Breed of Protest in a Networked World." *Boston College International and Comparative Law Review,* 35 (2): 511-542. Available at http://bit.ly/2EqJKET.

Hardy, Keiran & George Williams (2014). "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism." In Thomas M. Chen, Lee Jarvis & Stuart Macdonald (editors), *Cyberterrorism*, 1-23. New York: Springer.

Hua, Jian & Sanjay Bapna (2013). "The Economic Impact of Cyber Terrorism." *The Journal of Strategic Information Systems*, 22 (2): 175-186. DOI: 10.1016/j.jsis.2012.10.004.

Jakobs, Günther (2003). "Derecho penal del ciudadano y derecho penal del enemigo." In *Derecho penal del enemigo,* 19-56. Madrid: Civitas.

Jijena, Renato (2008). "Delitos informáticos, internet y derecho." In *Delito, pena y proceso*, 145-162. Santiago: Jurídica de Chile.

Jones, Andrew (2005). "Cyber Terrorism: Fact or Fiction." *Computer Fraud & Security*, 6: 4-7. DOI: 10.1016/S1361-3723(05)70220-7.

Kindhäuser, Urs (1989). *Gefährdung als Straftat*. Frankfurt: Vittorio Klostermann.

Kochheim, Dieter (2015). *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*. Munich: Beck.

Kraft, Ellen M. & Jinchang Wang (2009). "Effectiveness of Cyber bullying Prevention Strategies: A Study on Student's Perspectives." *International Journal of Cyber Criminology,* 3 (2): 513-535. Available at http://bit.ly/2EprLP7.

Lara, Juan Carlos, Manuel Martínez & Pablo Viollier (2014). "Hacia una regulación de los delitos informáticos basada en la evidencia." *Revista Chilena de Derecho y Tecnología*, 3 (1): 101-137. DOI: 10.5354/0719-2584.2014.32222.

Lewis, James Andrew (2002). "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." Center for Strategic & International Studies. Available at http://bit.ly/2Esfppx.

Madarie, Renushka (2017). "Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers." *International Journal of Cyber Criminology,* 11 (1): 78-97. DOI: 10.5281/zenodo.495773.

Mañalich, Juan (2015). "El terrorismo ante el derecho penal: la propuesta legislativa del gobierno como retroceso." *Anuario de Derecho Público UDP*, 6: 154-171.

—. (2017). "Terrorismo y organización." *Ius et Praxis*, 23 (1): 367-418. Available at http://bit.ly/2ErilCW.

Marberth-Kubicki, Annette (2010). *Computer- und Internetstrafrecht*. Munich: Beck.

Meier, Bernd-Dieter (2015). "Kriminologie und Internet: ein ungeklärtes Verhältnis." In Susanne Beck, Bernd-Dieter Meier, Carsten Momsen (editors), *Cybercrime und Cyberinvestigations*, 93-118. Baden-Baden: Nomos.

Melzer, Nils (2011). "Cyberwarfare and International Law." *Unidir Resources*, 1-38. Available at https://bit.ly/2UxGmwV.

Milan, Stefania & Arne Hintz (2013). "Networked Collective Action and the Institutionalized Policy Debate: Bringing Cyberactivism to the Policy Arena?" *Policy & Internet*, 5 (1): 7-26. DOI: 10.1002/poi3.20.

Mir Puig, Santiago (2016). *Derecho penal*: *Parte general*. 10.ª ed. Barcelona: Reppertor.

Miró Llinares, Fernando (2012). *El cibercrimen*. Madrid: Marcial Pons.

Neubacher, Frank (2014). *Kriminologie*. Baden-Baden: Nomos.

Podhradsky, Ashley, Rob D'Ovidio & Cindy Casey (2012). "The Xbox 360 and Steganography: How criminals and terrorists could be 'going dark'." *ADFSL Conference on Digital Forensics*, *Security and Law*, 33-51. Available at https://bit.ly/2EpvHiR.

Poveda Criado, Miguel Ángel & Begoña Torrente Barredo (2016). "Redes sociales y ciberterrorismo: Las TIC como herramienta terrorista." *Opción*, 32 (8): 509-518. Available at http://bit.ly/2EqqyqR.

Sorel, Jean-Marc (2003). "Some Questions About the Definition of Terrorism and the Fight Against its Financing." *European Journal of International Law*, 14 (2): 365-378. Available at http://bit.ly/2EqPJJR.

Teixeira, Adriano (2013). "Was ist böse am Terrorismus? Zugleich Vorüberlegungen zu einer Definition des Terrorismus." *Zeitschrift für Rechtsphilosophie*, 2: 57-76. Available at http://bit.ly/2EqrRWN.

Velásquez Velásquez, Fernando (2009). *Derecho penal*: *Parte general*. Volume 1. Santiago: Jurídica de Chile.

Villegas Díaz, Myrna (2016). "Contribuciones para un concepto de terrorismo en el derecho penal chileno." *Política Criminal*, 11 (21): 140-172. DOI: 10.4067/S0718-33992016000100006.

Von Bubnoff, Eckhart (2003). "Krimineller Missbrauch der neuen Medien im Spiegel europäischer Gegensteuerung." In *Strafrecht und Kriminalität in Europa*, 83-106. Baden-Baden: Nomos.

Von Hirsch, Andrew (1996). "Extending the Harm Principle: 'Remote' Harms and Fair Imputation." In Andrew Simester & Tony Smith (editors), *Harm and Culpability*, 259-276. Oxford: Clarendon Press. DOI: 10.1093/acprof:oso/9780198260578.003.0020.

Warren, Matthew (2008). "Terrorism and the Internet." In Lech J. Janczewsk & Andrew M. Colarik (editors), *Cyber Warfare and Cyber Terrorism,* 42-49. Hershey-New York: Information Science Reference.

Weimann, Gabriel (2005). "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism*, 28 (2): 129-149. DOI: 10.1080/10576100590905110.

Wilson, Clay (2003). "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." *CRS Report for Congress*. Available at https://bit.ly/2DRECsW.

Yannakogeorgos, Panayotis A. (2014). "Rethinking the Threat of Cyberterrorism." In Thomas M. Chen, Lee Jarvis & Stuart Macdonald (editors), *Cyberterrorism*, 43-62. New York: Springer.

About the author

Laura Mayer Lux es abogada. Licenciada en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, Chile. Doctora en Derecho por la Rheinische Friedrich Wilhelms-Universität Bonn, Alemania. Profesora de Derecho Penal de la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es laura.mayer@pucv.cl.

Laura Mayer Lux is a lawyer with a Degree in Legal Sciences from the Pontificia Universidad Católica de Valparaíso, Chile. PhD in Law from the Rheinische Friedrich Wilhelms-Universität Bonn, Germany. Professor of Criminal Law of the Pontificia Universidad Católica de Valparaíso. Her email is laura.mayer@pucv.cl.