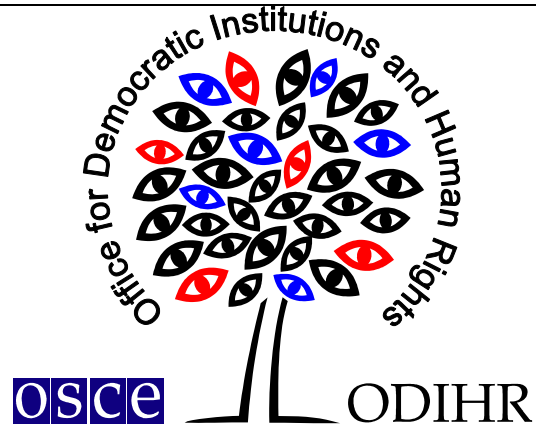


Warsaw, 27 March 2007

Opinion-Nr.:

FOI/TERR– UN/083/2007 (IU)

www.legislationline.org



**OSCE/ODIHR COMMENTS ON
LEGISLATIVE TREATMENT OF “CYBERTERROR”
IN DOMESTIC LAW OF INDIVIDUAL STATES**

TABLE OF CONTENTS:

1. INTRODUCTION

2. SCOPE OF REVIEW

3. STATEMENT OF ISSUE

4. COMPARATIVE TABLE

- Armenia
- Belarus
- Bulgaria
- Canada
- Croatia
- Denmark
- Estonia
- France
- Georgia
- Germany
- Israel
- Japan
- Korea
- Moldova
- Norway
- Poland
- Romania
- Russian Federation
- Serbia
- Slovakia
- Ukraine
- United Kingdom
- United States

1. INTRODUCTION

1. *On 12 March 2007, the OSCE/ODIHR was requested by the Strategic Planning Unit of the Executive Office of the Secretary General of the United Nations to produce a comparative outline of domestic legislative solutions regarding the use of the Internet for terrorist purposes. The requested document will be used by one of the working groups of the United Nations Counter-Terrorism Implementation Task Force (CTITF) focusing on the problem of countering the use of the Internet for terrorist purposes, in the development by the working group of concrete initiatives to implement key components of the United Nations Global Counter-Terrorism Strategy.*

2. SCOPE OF REVIEW

2. These Comments provide a brief analysis of the issue of “cyberterror” or “terrorism with the use of information technologies,” as well as map legislation from a selection of States both within and beyond the OSCE region to 5 main elements: (a) definition of terrorism; (b) measures against the use of computers and/or computer networks as tools and/or targets; (c) use of the IT as support for (physical) terrorist operations; (d) use of the Internet and electronic media in disseminating terrorist messages; and (d) regulation of the use of cryptography. The States have been selected based on the availability of relatively developed anti-terrorism and/or cybercrime legislation, as well as to ensure broad and balanced regional representation (EU, the Americas, South-East Europe, non-EU Eastern Europe, South Caucasus, Asia and the Pacific, Middle East).
3. These Comments follow the OSCE comprehensive approach to preventing and combating terrorism and take particular note of the Sofia Ministerial Council Decision 3/04 on Combating the Use of the Internet for Terrorist Purposes.¹
4. These Comments do not purport to provide a comprehensive review of individual States’ domestic legal frameworks concerning terrorism or cybercrime.
5. The OSCE/ODIHR would like to mention that the opinion provided herein is without prejudice to any further opinions or recommendations that the ODIHR may wish to make on the issue under consideration.

3. STATEMENT OF ISSUE

6. There is no universally accepted definition of “cyberterror” or “terrorism with the use of information technologies” and the working definitions put forward by individual agencies or researchers vary rather broadly.² In particular, while most

¹ The main OSCE documents outlining commitments to prevent and combat terrorism are the Bucharest Plan of Action (2001) and the OSCE Charter on Preventing and Combating Terrorism (2002). The OSCE/ODIHR in particular works to build awareness of human dimension issues in combating terrorism and to develop projects that fundamentally address factors engendering terrorism. Specifically, the OSCE/ODIHR has initiated programmes intended to promote human rights, build democratic institutions, and strengthen the rule of law as key components that enable states to address the various social, economic, political, and other factors that engender conditions in which terrorist and extremist organizations may recruit or win support.

² For instance, the U.S. Federal Emergency Management Agency (FEMA) definition reads as “*unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.*” The U.S. Federal Bureau of Investigation (FBI) defines cyberterrorism as “*any premeditated, politically motivated attack against information,*

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

sources agree that the perpetrators’ intent and/or motivation should be a key element in the definition,³ there is no consensus on the scale of effects of an act to qualify as “cyberterror,” nor on the means/mode of implementation (e.g. whether or not a physical attack against nodes in critical infrastructures would fall within the scope of “cyberterror”).⁴ Most of definitions also tend to exclude acts such as the criminal use of the Internet to finance terrorist operations (these would usually be viewed as general cybercrime), or purely as a means of communication support (e.g. through the use of the Internet-based telephony or chat software).

7. The OSCE approach has been to focus on the “use of the Internet for terrorist purposes” rather than on “cyberterror,” interpreting the former comprehensively as the use of the Internet by terrorist organizations “*to identify and to recruit potential members, to collect and transfer funds, to organize terrorist acts, to incite terrorist acts in particular through the use of propaganda.*”⁵
8. The potential implications of IT in terrorist activities (rather than “cyberterror”) are manifold and may be loosely grouped according to whether (a) it is digital property that is targeted by terrorists; or (b) IT is used as a support means in planning and organizing physical terrorist attacks; or (c) the cyberspace is used for disseminating terrorist statements and propaganda.
9. Based on this tentative classification, the following general framework may be developed for research on the potential uses of IT by terrorists:

1) Digital property as target:

- a) **Computer network attacks (cyberattacks):** Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks through unauthorized access, infecting with malicious code, and similar activities with primary reliance on data stream and not involving the use of physical force or electromagnetic energy;
- b) **Physical attacks:** Operations involving conventional weapons and directed against computers, computer networks and/or communication lines;
- c) **Electronic attacks:** Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks through the use of electromagnetic energy (such as EMP).

computer systems, computer programs, and data which results in violence against non-combatant objectives by sub-national groups or clandestine agents.” The U.S. National Infrastructure Protection Center (NIPC) defines it as “*a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the objective of influencing a government to conform to a particular political, social, or ideological agenda.*”

³ The same is to a certain extent true also with regard to the notion of “terrorism” in general, since no single universal definition has been adopted so far, and the existing definitions do vary to some degree.

⁴ *Cp.* the FEMA definition (*see* Footnote 2) which would cover physical and electronic attacks as well, and the NIPC definition (*id.*) which is restricted to computer network attacks (and possibly electronic attacks, e.g. when a malicious code is inserted into radio transmission).

⁵ See the OSCE Sofia Ministerial Council Decision 3/04, Combating the Use of the Internet for Terrorist Purposes.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

2) IT as a support means in terrorist operations:

- a) *Use of the IT-based communication means* while planning, preparing or organizing terrorist attacks; also the *use of cryptography*;
- b) *Intelligence collection through unauthorized access*;
- c) *Use of information networks to provide financial support for terrorist activities*.

3) Cyberspace as a channel for disseminating terrorist messages:

- a) *Dissemination of terrorist propaganda*;
- b) *Dissemination of terrorist statements intended to inculcate fear* (including hate speech).

10. The Comparative Table (see the next Section) is based on the above framework and does not focus exclusively on what would be viewed as “cyberterror” by most specialists. It maps legislation from a selection of OSCE participating as well as Partner for Cooperation States⁶ to the 5 main components of the framework: (a) definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT; (b) measures against the use of computers and/or computer networks as tools and/or targets; (c) use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.); (d) use of the Internet and electronic media in disseminating terrorist messages, including propaganda; and (d) regulation of the use of cryptography⁷ (understood broadly and including encryption, steganography, password-protected files etc.). The States have been selected based on the availability of relatively developed anti-terrorism and/or cybercrime legislation, as well as to ensure broad and balanced regional representation (EU, the Americas, South-East Europe, non-EU Eastern Europe, South Caucasus, Asia and the Pacific, Middle East).

⁶ Armenia, Belarus, Bulgaria, Canada, Croatia, Denmark, Estonia, France, Georgia, Germany, Israel, Japan, Korea, Moldova, Norway, Poland, Romania, Russian Federation, Serbia, Slovakia, Ukraine, United Kingdom, United States. OSCE participating States: Armenia, Belarus, Bulgaria, Canada, Croatia, Denmark, Estonia, France, Georgia, Germany, Moldova, Norway, Poland, Romania, Russian Federation, Serbia, Slovakia, Ukraine, United Kingdom, United States. OSCE Partner for Cooperation States: Israel, Japan, Korea.

⁷ Albeit not an OSCE participating State nor a Partner for Cooperation, and therefore not included in the comparative table that follows, the case of India merits particular attention in connection with the use of cryptography, since India is one of the countries with very detailed regulation of cryptography in particular through a licensing regime for the import and export of cryptography. In addition, India’s law stipulates for the office of the Controller of Certifying Authorities with the authority to direct any Government agency to intercept any information transmitted through any computer resource. (See India’s Information Technology Act 2000 and relevant regulations for more information).

4. COMPARATIVE TABLE

ARMENIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Law on Combating Terrorism</p> <p>Article 5. Main Concepts Used in the Law</p> <p>The following main concepts shall be used in this law:</p> <p>1) Act of terrorism: direct commission of an offence of terrorist nature via an explosion, arson, use or the threat to use nuclear explosive, radioactive, chemical, biological, explosive, toxic, virulent or poisonous substances, destruction or seizure of or damage to the means of transport or other objects, trespassing against any state or public official, any representative of a national, ethnic, religious or other social group, causing a danger to the life, health or property of any person by means of taking hostages, kidnapping of humans, <u>creation of conditions supportive of technogen accidents and disasters or causing a real</u></p>	<p>Criminal Code</p> <p>Article 252. Modification of computer information.</p> <p>1. Modification of information stored in a computer, computer system, network or on storage media, or entering obviously false information therein, in the absence of elements of property theft, or infliction of property damage by deception or abuse of confidence, which caused significant damage, is punished with a fine in the amount of 200 to 500 minimal salaries, or with correctional labor for the term of up to 1 year.</p> <p>2. The same action which:</p> <p>1) was accompanied with access (penetration) into a computer system or</p>	<p>Criminal Code</p> <p>Article 254. Illegal appropriation of computer data.</p> <p>1. Copying or appropriating in any other way, of computer data stored in the computer system, network or on storage media, interception of transmitted data by means of computer communication, is punished with a fine in the amount of 200 to 400 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years.</p> <p>2. Forcing the submission of</p>	<p>Criminal Code</p> <p>Article 254. Illegal appropriation of computer data.</p> <p>1. Copying or appropriating in any other way, of computer data stored in the computer system, network or on storage media, interception of transmitted data by means of computer communication, is punished with a fine in the amount of 200 to 400 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years.</p> <p>2. Forcing the submission of</p>	<p>Criminal Code</p> <p>Article 255. Manufacture or sale of special devices for illegal penetration into a computer system or network.</p> <p>Manufacture of special hardware or software for the illegal penetration into a protected computer system or network for the purpose of sale, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years.</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p><u>threat of such a danger, spreading threats by any means</u>, human victims, significant damage to the property or other acts entailing dangerous consequences for the public.</p> <p>Criminal Code</p> <p>Article 217. Terrorism.</p> <p>1. Terrorism, i.e. committal of explosion, arson or actions causing significant human losses, <u>or other actions inflicting significant damage to property or actions causing danger to public, or threat of such actions</u>, if these actions were committed with the purpose of violation of public security, intimidation of the population or exerting pressure on decision making by a state official, as well as, for the purpose of fulfilling another demand of the perpetrator, is punished with imprisonment for the term of 5 to 10 years.</p> <p>2. The same action committed</p> <p>1) by a several persons with prior agreement,</p> <p>2) using firearms, is punished with imprisonment for the term of 8 to 12 years.</p> <p>3. Actions envisaged in parts 1 or 2 of this</p>	<p>network without permission;</p> <p>2) was committed by abuse of official position,</p> <p>3) was committed by a group with prior agreement,</p> <p>4) negligently caused grave consequences,</p> <p>is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3 months, or with imprisonment for the term of up to 2 years.</p> <p>Article 253. Computer sabotage.</p> <p>1. Obliteration (sabotage) of computer data or software, isolation or making it unusable, spoilage of computer equipment or destruction of the computer system, network or on storage media, is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 1 year, or with arrest for the term of 1-3, or with imprisonment for the term of up to 2 years.</p> <p>2. The same action:</p>	<p>data mentioned in part 1 of this Article stored in the computer system, network or on storage media, by threat of publicizing defamatory information concerning a person or his close relatives, facts which the aggrieved wishes to keep secret, or with a threat to use violence against the person or his relatives, or against the person who manages this information, with a threat to destroy or damage the property, is punished with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3, or with imprisonment for 2-5 years.</p> <p>3. Actions envisaged in parts 1 or 2 of this Article which:</p> <p>1) were accompanied with use of violence against the person or his close relatives;</p> <p>2) were committed by a group with prior agreement;</p> <p>3) inflicted significant damage to the aggrieved;</p> <p>4) were committed with the</p>	<p>data mentioned in part 1 of this Article stored in the computer system, network or on storage media, by threat of publicizing defamatory information concerning a person or his close relatives, facts which the aggrieved wishes to keep secret, <u>or with a threat to use violence against the person or his relatives, or against the person who manages this information, with a threat to destroy or damage the property</u>, is punished with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3, or with imprisonment for 2-5 years.</p> <p>3. Actions envisaged in parts 1 or 2 of this Article which:</p> <p>1) were accompanied with use of violence against the person or his close relatives;</p> <p>2) were committed by a group with prior agreement;</p> <p>3) inflicted significant damage to the aggrieved;</p> <p>4) were committed with the</p>	
---	--	---	---	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>Article, if they were committed:</p> <p>1) by an organized group;</p> <p>2) were accompanied with use of mass destruction weapon, radioactive materials or with a threat to use other means causing mass losses,</p> <p>3) caused death by negligence or other grave consequences, is punished with imprisonment for the term of 10 years to 15 years.</p> <p>3. A person who participated in terrorism is exempted from criminal liability if he advised the authorities on time, or otherwise, contributed into the prevention of terror act, and if his actions do not contain the elements of other crime.</p> <p>Article 219. Occupation of buildings, facilities, means of transportation or <u>communication</u>.</p> <p>1. Occupation of buildings, facilities, means of transportation and communication, other communication lines, or keeping them, accompanied with a threat of their destruction or damage, which was committed to force the state, an organization or a citizen to perform or not to perform certain action on condition of vacating the occupied property, is punished with imprisonment for the term of</p>	<p>1) accompanied with access (penetration) into a computer system or network without permission;</p> <p>2) negligently caused grave consequences,</p> <p>is punished with correctional labor for the term of up to 2 years, or with imprisonment for the term of up to 4 years.</p> <p>3. The acts envisaged in part 1 or 2 of this Article which <u>willfully caused severe consequences</u>, are punished with imprisonment for 3-6 years.</p> <p>[...]</p> <p>Article 256. Manufacture, use and dissemination of hazardous software.</p> <p>1. Development of computer software for the purpose of obliteration, isolation, changing of data stored in the computer system, network or on storage media, or for making changes in existing software, or developing software with special viruses, their use, or dissemination of storage media with such software, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of 1-3, or with</p>	<p>purpose of obtaining particularly valuable information,</p> <p>are punished with imprisonment for the term of 4 to 10 years.</p> <p>4. Actions envisaged in parts 1, 2 or 3 of this Article which:</p> <p>1) were committed by an organized group;</p> <p>2) were accompanied with infliction of damage to health or other grave consequences,</p> <p>are punished with imprisonment for the term of 6 to 12 years.</p>	<p>purpose of obtaining particularly valuable information,</p> <p>are punished with imprisonment for the term of 4 to 10 years.</p> <p>4. Actions envisaged in parts 1, 2 or 3 of this Article which:</p> <p>1) were committed by an organized group;</p> <p>2) were accompanied with infliction of damage to health or other grave consequences,</p> <p>are punished with imprisonment for the term of 6 to 12 years.</p>	
---	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>up to 5 years.</p> <p>2. The same action which is committed:</p> <p>1) By a group with prior agreement;</p> <p>2) by threatening violence dangerous for life or health;</p> <p>3) by using weapons or other items as weapons, is punished with imprisonment for the term of 4 to 10 years.</p> <p>3. Actions envisaged in parts 1 or 2 of this Article, if they were committed:</p> <p>1) by an organized group;</p> <p>2) caused death by negligence or damage to health, is punished imprisonment for the term of 6 years to 12 years.</p> <p>4. The person who refused from one’s demands who vacated voluntarily the occupied property is exempted from criminal liability, if his actions do not contain other elements of crime.</p>	<p>imprisonment for the term of up to 2 years and a fine in the amount of 100 to 300 minimal salaries.</p> <p>2. The same action,</p> <p>1) Committed with mercenary motives,</p> <p>2) Committed by a group with prior agreement,</p> <p>3) which negligently caused grave consequences, is punished with imprisonment for the term of 2 to 5 years.</p>			
---	---	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

BELARUS

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Law on Combating Terrorism</p> <p>Article 3.</p> <p>[...]</p> <p>terrorism - perpetrating an explosion, arson attack or other actions which create the danger of the loss of human life, bodily harm, cause widespread damage or the onset of other serious consequences with the aim of causing public panic or exerting influence on decision-making by government bodies or hindering political or other public activity, and also threatening to carry out such activity with the same aims; attempt on the life of a government or public official carried out in connection with his government or public activities with the aim of destabilising public order or exerting influence on decision-making of government bodies or hindering political or other public activity, or out of revenge for such activity; the organisation or actual perpetration of an explosion, arson</p>	<p>Criminal Code</p> <p>Section XII. Chapter 31. Crimes against information security</p> <p>Article 349. Unauthorized access to computer information</p> <p>1. Unauthorized access to information in the computer system, network or on the machine carriers accompanied with breaking their protecting means and resulted in imprudently erasing, blocking, modifying information or putting computer equipment out of action, or caused another considerable damage is punished with fine or arrest within up to six months.</p> <p>2. The same action carried out for mercenary purpose, either by a group of persons in prior agreement or a person having an access to computer system or network is punished with fine, denial of particular position or activity privileges, arrest within the term from three to six months, freedom limitation within up to two years or imprisonment within the</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>attack or other actions on the territory of a foreign state with the purpose of killing people or causing them grievous bodily harm, <u>destruction or damage to</u> buildings, installations, <u>ways and means of communication</u> or other property with the aim of provoking international complications, war or destabilisation of the domestic situation in these states, or the murder or grievous bodily harm of government or public officials of foreign states or damage to their property with the same aims.</p>	<p>same term.</p> <p><u>3. Unauthorized access to computer information or use of electronic computers, their system or network entailed [that has resulted in? Author’s note] imprudently wreck, breakdown, disaster, accidents, negative environmental changes or other grave consequences are punished with freedom limitation within up to five years or imprisonment within up to seven years.</u></p> <p>Article 351. Computer sabotage Intentional deletion, blocking, destruction of computer information or programs and damage of computers, their systems, networks or machine carriers (computer sabotage) are punished with fine, denial of particular position or activity privileges, arrest within the term from three to six months, freedom limitation within up to five years or imprisonment within the term from one to five years.</p> <p><u>2. Computer sabotage connected with unauthorized access to computer system or network entailed grave consequences is punished with imprisonment within the term from three to ten years.</u></p>			
---	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org> and http://www.crime-research.org/library/Criminal_Codes.html.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

BULGARIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Criminal Code</p> <p>Art. 319a (1) A person who obtains unauthorized access to the resources of a computer and copies or uses computer data without permission, when such one is required shall be punished with a fine of up to 3,000 lev.</p> <p>(2) In case the act under para one has been committed by two or more persons that have conspired to commit the act, the punishment shall be imprisonment up to one year or a fine of up to 3,000 lev.</p> <p>(3) In case the act under para one is committed repeatedly the punishment shall be imprisonment of up to three years or a fine of up to 5,000 lev.</p> <p>(4) If the acts under the previous items 1-3 are committed concerning information qualified as government secret, the punishment shall be imprisonment from one to three years, provided there is no heavier punishment prescribed.</p> <p>(5) If the act under item four causes grave</p>			<p>Criminal Code</p> <p>Art. 319e (1) A person who distributes computer or system password and this results in disclosure of personal data or a government secret shall be punished with imprisonment up to one year.</p> <p>(2) If the act under the previous paragraph has been committed for material advantage or has caused significant damage, the punishment shall be imprisonment up to three years.</p> <p>Art. 319f A service provider who violates the provisions of Art. 6, para 2, item 5 of the Electronic Document and Electronic Signature Act</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>consequences, the punishment shall be imprisonment from one to eight years.</p> <p>Art. 319b (1) A person who without the permission of the administrator or the user of the computer adds, changes, deletes or destroys a computer program or data when the impact is significant shall be punished with imprisonment up to one year or a fine up to 2,000 lev.</p> <p>(2) In case the act under the previous paragraph has caused significant damage or other grave consequences, the punishment shall be imprisonment up to two years or a fine of 3,000 lev.</p> <p>(3) In case the act under para one has been committed with the purpose of obtaining material benefit the punishment shall be imprisonment from one up to three years or a fine of 5,000 lev.</p> <p>Art. 319c (1) A person who commits an act under the previous article with regard to data that by virtue of a law are provided through electronic means or through a magnetic carrier shall be punished by imprisonment of up to two year and fine of up to 3 000 lev.</p> <p><u>(2) If the act under the previous para has been committed for the purpose of frustrating the execution of duties,</u> the punishment shall be imprisonment up to three years and a fine of up to 5,000 lev.</p>			<p>shall be punished with a fine of up to 5,000 lev, provided he is not punishable with a heavier punishment.</p>
--	---	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>Art. 319d (1) A person who brings a computer virus in a computer or the information network shall be punished with a fine of up to 3,000 lev.</p> <p>(2) <u>If significant damage has been caused by the act under the previous paragraph</u> or it has been committed repeatedly the punishment shall be imprisonment up to three years and a fine of up to one thousand lev.</p>			
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/bulgaria.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

CANADA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Criminal Code</p> <p>Part II.1: Terrorism</p> <p>(b) an act or omission, in or outside Canada,</p> <p>(i) that is committed</p> <p>(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and</p> <p>(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and</p> <p>(ii) that intentionally</p>	<p>Criminal Code</p> <p>342.1 (1) Every one who, fraudulently and without color of right,</p> <p>(a) obtains, directly or indirectly, any computer service,</p> <p>(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system.</p> <p>(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or</p> <p>(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)</p> <p>is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an</p>			<p>Criminal Code</p> <p>342.1 (1) Every one who, fraudulently and without color of right,</p> <p>(a) obtains, directly or indirectly, any computer service,</p> <p>(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system.</p> <p>(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or</p> <p>(d) uses, possesses, traffics</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>(A) causes death or serious bodily harm to a person by the use of violence,</p> <p>(B) endangers a person’s life,</p> <p>(C) causes a serious risk to the health or safety of the public or any segment of the public,</p> <p>(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or</p> <p>(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),</p> <p>and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counseling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of</p>	<p>offence punishable on summary conviction.</p> <p>342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,</p> <p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or</p> <p>(b) is guilty of an offence punishable on summary conviction.</p> <p>430. (1.1) Every one commits mischief who wilfully</p> <p>(a) destroys or alters data;</p> <p>(b) renders data meaningless, useless or ineffective;</p> <p>(c) obstructs, interrupts or interferes with the lawful use of data; or</p> <p>(d) obstructs, intercepts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.</p>			<p><u>in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)</u> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.</p>
---	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.				
---	--	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/canada.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

CROATIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Criminal Code</p> <p>Anti-State Terrorism</p> <p>Article 141</p> <p>Whoever, with an aim to endanger the constitutional order or the security of the Republic of Croatia, causes an explosion, fire, or by a generally dangerous act or device imperils the lives of people or endangers property or kidnaps a person, or commits some other act of violence within the territory of the Republic of Croatia or against its citizens, thus causing a feeling of personal insecurity in citizens, shall be punished by imprisonment for not less than three years.</p> <p>[...]</p> <p>Act of Sabotage</p>	<p>Criminal Code</p> <p>Article 223. Damage to secrecy integrity and availability of computer data, programmes or systems</p> <p>(1) Whoever, despite protective measures and without authorisation accesses a computer system shall be punished by a fine or by imprisonment up to one year.</p> <p>(2) Whoever with an aim to disable or renders unusable work or use of computer data or programmes, a computer system or computer communication shall be punished with a fine or imprisonment up to three years.</p> <p>(3) Whoever without being authorised damages, alters, deletes, destroys or renders in any way unusable or unavailable other people’s computer data or programmes shall be punished by penalty from paragraph two of this</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>Article 143</p> <p>Whoever, with an aim to endanger the constitutional order or the security of the Republic of Croatia, by way of demolition, fire or in some other way <u>destroys or damages</u> an industrial, agricultural or other economic facility or a plant, a road, a means of transport, <u>a communication device</u>, heating, gas, electric or some other power installation, a dam or any other facility, plant <u>or installation of importance for the everyday life of citizens</u> shall be punished by imprisonment for not less than three years.</p>	<p>article.</p> <p>(4) Whoever intercepts or records a non-public transmission of computer data towards the computer system, from with or within it, including electromagnetic emissions of the computer system that is transmitting this data that are not meant for him, or whoever introduces this data to an uninvited person shall be punished by penalty from paragraph two of this article.</p> <p><u>(5) If the criminal offence as stated in article 1., 2., 3. or 4. of this article is committed related to a computer data, programme or a government authority system, public institution or a company of special public interest, or if significant damage was caused,</u> the perpetrator shall be punished by imprisonment from three months to five years.</p>			
---	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

DENMARK

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Penal Code</p> <p>§ 193. (1) Any person who, in an unlawful manner, causes major disturbances in the operation of public means of communication, of the public mail service, of publicly used telegraph or telephone services, of radio and television installations, of information systems or of installations for public supply of water, gas, electricity or heating shall be liable to imprisonment not exceeding 6 years or to a fine.</p>			

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/denmark.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

ESTONIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Criminal Code</p> <p>§ 206. Computer sabotage (1) Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, if significant damage is thereby caused, or unlawful entry of data or programs in a computer, if significant damage is thereby caused, is punishable by a pecuniary punishment or up to one year of imprisonment. (2) The same act, if committed with the intention to interfere with the work of a computer or telecommunications system, is punishable by a pecuniary punishment or up to 3 years' imprisonment.</p> <p>§ 207. Damaging of connection to computer network Damaging or obstructing a connection to a computer network or computer system is punishable by a pecuniary punishment.</p> <p>§ 208. Spreading of computer viruses</p>			<p>Criminal Code</p> <p>§ 284. Handing over protection codes Unlawfully handing over the protection codes of a computer, computer system or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences is punishable by a pecuniary punishment or up to 3 years imprisonment.</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>(1) Spreading of a computer virus is punishable by a pecuniary punishment or up to one year of imprisonment.</p> <p>(2) The same act, if committed:</p> <p>1) at least twice, or</p> <p>2) in a manner which causes significant damage,</p> <p>is punishable by a pecuniary punishment or up to 3 years’ imprisonment.</p> <p>§ 217. Unlawful use of computer, computer system or computer network</p> <p>(1) Unlawful use of a computer, computer system or computer network by way of removing a code, password or other protective measure is punishable by a pecuniary punishment.</p> <p>(2) <u>The same act, if it:</u></p> <p><u>1) causes significant damage, or</u></p> <p><u>2) is committed by using a state secret or a computer, computer system or computer network containing information prescribed for official use only,</u></p> <p>is punishable by a pecuniary punishment or up to 3 years imprisonment.</p>			
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/estonia.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

FRANCE

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Penal Code</p> <p>TITLE II. - OF TERRORISM</p> <p>CHAPTER I. - OF ACTS OF TERRORISM</p> <p>Article 421-1</p> <p>The following offences constitute acts of terrorism where they are committed intentionally in connection with an individual or collective undertaking the purpose of which is seriously to disturb the public order through intimidation or terror:</p> <p>[...]</p> <p><u>2° theft, extortion, destruction, defacement and damage, and also computer offences, as defined under Book III of the present Code.</u></p>	<p>Penal Code</p> <p>(as amended by Loi Godfrain /Loi n° 88-19 du 5 Janvier 1988/ and Loi du Loi du 21 juin 2004 pour la confiance dans l'économie numérique</p> <p>21 juin 2004 pour la confiance dans l'économie numérique)</p> <p>Article 323-1: Fraudulent accessing or remaining within all or part of an automated data processing system is punished by a sentence not exceeding two years' imprisonment and a fine of 30,000 Euro.</p> <p>Where this behavior causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is not exceeding three years'</p>			<p>Loi du 21 juin 2004 pour la confiance dans l'économie numérique</p> <p>DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE</p> <p>CHAPITRE Ier Moyens et prestations de cryptologie</p> <p>Article 29</p> <p>On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>imprisonment and a fine of 45,000 Euro.</p> <p>Article 323-2 Obstruction or interference with the functioning of an automated data processing system is punished by a sentence not exceeding five years’ imprisonment and a fine of 75,000 Euro.</p> <p>Article 323-3 The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine of 75,000 Euro.</p> <p>Article 323-3-1 Fraudulently, and without legitimate motive, importing, holding, offering, selling or making available any equipment, tool, computer program or any data designed or particularly adapted to commit one or more offences provided for by articles 323-1 to 323-3, is punishable by the sentences prescribed for offences in preparation or the one that carries the heaviest penalty.</p> <p>Article 323-4 <u>The participation in a group or conspiracy established with a view to the preparation of one or more</u></p>			<p>secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d’assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.</p> <p>On entend par prestation de cryptologie toute opération visant à la mise en oeuvre, pour le compte d’autrui, de moyens de cryptologie.</p> <p>Section 1</p> <p>Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie</p> <p>Article 30</p> <p>I. - L’utilisation des moyens de cryptologie est libre.</p> <p>II. - La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l’importation et l’exportation</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p><u>offences set out under articles 323-1 to 323-3, and demonstrated by one or more material actions,</u> is punished by the penalties prescribed for offences in preparation or one that carries the heaviest penalty.</p>			<p>des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres.</p> <p>III. - La fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au b du présent III. Le fournisseur ou la personne procédant au transfert ou à l'importation tiennent à la disposition du Premier ministre une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. Un décret en Conseil d'Etat fixe:</p> <p>a) Les conditions dans lesquelles sont souscrites ces déclarations, les conditions</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>et les délais dans lesquels le Premier ministre peut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques;</p> <p>b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis un Etat membre de la Communauté européenne ou leur importation peuvent être dispensés de toute formalité préalable.</p> <p>IV. - Le transfert vers un Etat membre de la Communauté européenne et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier ministre, sauf dans les cas prévus au b du présent IV. Un décret en</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>Conseil d'Etat fixe:</p> <p>a) Les conditions dans lesquelles sont souscrites les demandes d'autorisation ainsi que les délais dans lesquels le Premier ministre statue sur ces demandes;</p> <p>b) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur transfert vers un Etat membre de la Communauté européenne ou leur exportation peuvent être soit soumis au régime déclaratif et aux obligations d'information prévus au III, soit dispensés de toute formalité préalable.</p> <p>Section 2 Fourniture de prestations de cryptologie</p> <p>Article 31</p> <p>I. - La fourniture de</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>prestations de cryptologie doit être déclarée auprès du Premier ministre. Un décret en Conseil d'Etat définit les conditions dans lesquelles est effectuée cette déclaration et peut prévoir des exceptions à cette obligation pour les prestations dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, cette fourniture peut être dispensée de toute formalité préalable.</p> <p>II. - Les personnes exerçant cette activité sont assujetties au secret professionnel, dans les conditions prévues aux articles 226-13 et 226-14 du code pénal.</p> <p>Article 32</p> <p>Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.</p> <p>Article 33</p> <p>Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants:</p> <p>1° Les informations contenues dans le certificat, à la date de sa délivrance,</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>étaient inexactes;</p> <p>2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes;</p> <p>3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat;</p> <p>4° Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.</p> <p>Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>utilisateurs.</p> <p>Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.</p> <p>Section 3 Sanctions administratives</p> <p>Article 34</p> <p>Lorsqu'un fournisseur de moyens de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujéti en application de l'article 30, le Premier ministre peut, après avoir mis l'intéressé à même de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>cryptologie concerné.</p> <p>L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur l'obligation de procéder au retrait:</p> <p>1° Auprès des diffuseurs commerciaux, des moyens de cryptologie dont la mise en circulation a été interdite;</p> <p>2° Des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de diffuseurs commerciaux.</p> <p>Le moyen de cryptologie concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues à l'article 30.</p> <p>Section 4</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>Dispositions de droit pénal</p> <p>Article 35</p> <p>I. - Sans préjudice de l'application du code des douanes:</p> <p>1° Le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 30 en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au Premier ministre prévue par ce même article est puni d'un an d'emprisonnement et de 15 000 e d'amende;</p> <p>2° Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un Etat membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30 ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et de 30</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>000 e d'amende.</p> <p>II. - Le fait de vendre ou de louer un moyen de cryptologie ayant fait l'objet d'une interdiction administrative de mise en circulation en application de l'article 34 est puni de deux ans d'emprisonnement et de 30 000 e d'amende.</p> <p>III. - Le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 31 est puni de deux ans d'emprisonnement et de 30 000 e d'amende.</p> <p>IV. - Les personnes physiques coupables de l'une des infractions prévues au présent article encourent également les peines complémentaires suivantes:</p> <p>1° L'interdiction, suivant les modalités prévues par les articles 131-19 et 131-20 du code pénal, d'émettre des chèques autres que ceux qui</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés, et d'utiliser des cartes de paiement;</p> <p>2° La confiscation, suivant les modalités prévues par l'article 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution;</p> <p>3° L'interdiction, suivant les modalités prévues par l'article 131-27 du code pénal et pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise;</p> <p>4° La fermeture, dans les conditions prévues par l'article 131-33 du code pénal et pour une durée de cinq ans au plus, des</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;</p> <p>5° L'exclusion, dans les conditions prévues par l'article 131-34 du code pénal et pour une durée de cinq ans au plus, des marchés publics.</p> <p>V. - Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions prévues au présent article. Les peines encourues par les personnes morales sont:</p> <p>1° L'amende, suivant les modalités prévues par l'article 131-38 du code pénal;</p> <p>2° Les peines mentionnées à l'article 131-39 du code pénal.</p> <p>VI. - L'article L. 39-1 du code des postes et</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>télécommunications est complété par un 4° ainsi rédigé:</p> <p>« 4° De commercialiser ou de procéder à l'installation d'appareils conçus pour rendre inopérants les téléphones mobiles de tous types, tant pour l'émission que pour la réception, en dehors des cas prévus à l'article L. 33-3. »</p> <p>Article 36</p> <p>Outre les officiers et agents de police judiciaire agissant conformément aux dispositions du code de procédure pénale et, dans leur domaine de compétence, les agents des douanes agissant conformément aux dispositions du code des douanes, les agents habilités à cet effet par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat peuvent rechercher et constater par procès-verbal les infractions aux dispositions des articles 30,</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>31 et 34 de la présente loi et des textes pris pour leur application.</p> <p>Les agents habilités par le Premier ministre mentionnés à l’alinéa précédent peuvent accéder aux moyens de transport, terrains ou locaux à usage professionnel, à l’exclusion des parties de ceux-ci affectées au domicile privé, en vue de rechercher et de constater les infractions, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications. Les agents ne peuvent accéder à ces locaux que pendant leurs heures d’ouverture lorsqu’ils sont ouverts au public et, dans les autres cas, qu’entre 8 heures et 20 heures.</p> <p>Le procureur de la République est préalablement informé des opérations envisagées en vue de la recherche des infractions. Il peut s’opposer</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>à ces opérations. Les procès-verbaux lui sont transmis dans les cinq jours suivant leur établissement. Une copie en est également remise à l'intéressé.</p> <p>Les agents habilités peuvent, dans les mêmes lieux et les mêmes conditions de temps, procéder à la saisie des moyens de cryptologie mentionnés à l'article 29 sur autorisation judiciaire donnée par ordonnance du président du tribunal de grande instance ou d'un magistrat du siège délégué par lui, préalablement saisi par le procureur de la République. La demande doit comporter tous les éléments d'information de nature à justifier la saisie. Celle-ci s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée.</p> <p>Les matériels et logiciels saisis sont immédiatement inventoriés. L'inventaire est annexé au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>de l'inventaire sont transmis, dans les cinq jours suivant leur établissement, au juge qui a ordonné la saisie. Ils sont versés au dossier de la procédure.</p> <p>Le président du tribunal de grande instance ou le magistrat du siège délégué par lui peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner mainlevée de la saisie.</p> <p>Est puni de six mois d'emprisonnement et de 7 500 € d'amende le fait de faire obstacle au déroulement des enquêtes prévues au présent article ou de refuser de fournir les informations ou documents y afférant.</p> <p>Article 37</p> <p>Après l'article 132-78 du code pénal, il est inséré un article 132-79 ainsi rédigé:</p> <p>« Art. 132-79. - Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin</p>
--	--	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit:</p> <p>« 1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle;</p> <p>« 2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle;</p> <p>« 3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle;</p> <p>« 4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>d'emprisonnement;</p> <p>« 5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement;</p> <p>« 6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement;</p> <p>« 7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.</p> <p>« Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement. »</p> <p>Section 5 Saisine des moyens de l'Etat pour la mise au clair de</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>données chiffrées</p> <p>Article 38</p> <p>Après le premier alinéa de l'article 230-1 du code de procédure pénale, il est inséré un alinéa ainsi rédigé:</p> <p>« Si la personne ainsi désignée est une personne morale, son représentant légal soumet à l'agrément du procureur de la République ou de la juridiction saisie de l'affaire le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques mentionnées au premier alinéa. Sauf si elles sont inscrites sur une liste prévue à l'article 157, les personnes ainsi désignées prêtent, par écrit, le serment prévu au premier alinéa de l'article 160. »</p> <p>Section 6 Dispositions diverses</p> <p>Article 39</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>Les dispositions du présent chapitre ne font pas obstacle à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, à ceux des moyens de cryptologie qui sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en oeuvre les armes, soutenir ou mettre en oeuvre les forces armées, ainsi qu'à ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale.</p> <p>Article 40</p> <p>I. - L'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications est abrogé à compter de l'entrée en vigueur du présent chapitre.</p> <p>II. - Les autorisations et déclarations de fourniture, d'importation et d'exportation de moyens de</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				<p>cryptologie délivrées ou effectuées conformément aux dispositions de l'article 28 de la loi n° 90-1170 du 29 décembre 1990 précitée et de ses textes d'application conservent leurs effets jusqu'à l'expiration du terme prévu par celles-ci. Les agréments délivrés aux organismes chargés de gérer pour le compte d'autrui des conventions secrètes de moyens de cryptologie permettant d'assurer des fonctions de confidentialité valent, pour ces moyens, déclaration au sens de l'article 31.</p>
--	--	--	--	---

Source(s): The quoted legislation available at <http://www.legislationline.org> and <http://www.mentions-legales.fr/html/lcen.php>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

GEORGIA

<p>Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT</p>	<p>Measures against the use of computers and/or computer networks as tools and/or targets</p>	<p>Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)</p>	<p>Use of the Internet and electronic media in disseminating terrorist messages, including propaganda</p>	<p>Regulation of the use of cryptography</p>
<p>Criminal Code</p> <p>Article 324(1). Cyberterrorism</p> <p>1. Cyberterrorism, i.e. unlawful possession, use or threat to use of computerized information protected by law, that poses a threat of grave consequences and undermines public security, strategic, political or economic interest, perpetrated to intimidate the population and/or put pressure upon a governmental body</p> <p>- shall be punishable by deprivation of liberty from ten to fifteen years.</p> <p>2. Same act that caused a death or any other grave consequences,</p> <p>- shall be punishable by deprivation of liberty from twelve to twenty years or to life imprisonment.</p>	<p>Criminal Code</p> <p>Article 324(1). Cyberterrorism</p> <p>1. Cyberterrorism, i.e. unlawful possession, use or threat to use of computerized information protected by law, that poses a threat of grave consequences and undermines public security, strategic, political or economic interest, perpetrated to intimidate the population and/or put pressure upon a governmental body</p> <p>- shall be punishable by deprivation of liberty from ten to fifteen years.</p> <p>2. Same act that caused a death or any other grave consequences,</p> <p>- shall be punishable by deprivation of liberty from twelve to twenty years or to life imprisonment.</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

GERMANY

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Criminal Code</p> <p>Section 202a. Data Espionage: (1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine. (2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.</p> <p>Section 303a. Alteration of Data (1) Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine. (2) The attempt shall be punishable.</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>Section 303b. Computer Sabotage (1) Imprisonment not exceeding five years or a fine shall be imposed on <u>any person who interferes with data processing which is of essential importance to another business, another's enterprise or an administrative authority</u> by:</p> <ol style="list-style-type: none">1. committing an offense under section 300a(1) or2. destroying, damaging, rendering useless, removing, or altering a computer system or a data carrier. <p>(2) The attempt shall be punishable.</p>			
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/germany.html>.

ISRAEL

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Prohibition on Terrorist Financing Law, 5765-2004</p> <p>Chapter One: Interpretation</p> <p>Definitions</p> <p>“An act of terrorism” –</p> <p>(a) an act that constitutes an offence or a threat to commit an act that constitutes an offence that was committed or was planned to be committed in order to influence a matter of policy, ideology or religion if all of the following conditions are fulfilled:</p> <p>(1) it was committed or was planned to be committed with the goal of causing fear or panic among the public or with the goal of coercing a government or another governing authority, including the government or governing authority of a foreign country to take action or to refrain from taking action; for the purposes of this</p>	<p>The Computers Law of 1995</p> <p>CHAPTER TWO: COMPUTER OFFENSES</p> <p>Damage to or disruption of computer or computer material</p> <p>2. If a person unlawfully committed any of the following, he shall be liable to three years imprisonment:</p> <p>(1) he disrupted the orderly operation of a computer or interfered with its use;</p> <p>(2) he erased computer material, caused an alteration of it, disrupted it in any other manner or interfered with its use.</p> <p>Penetration of computer material</p> <p>4. If a person unlawfully penetrated computer material in a computer, then he shall be liable to three years imprisonment; for this purpose, “penetration of computer material” – penetration by means of communication, by connection to the computer, or by its</p>	<p>The Computers Law of 1995</p> <p>CHAPTER TWO: COMPUTER OFFENSES</p> <p>[...]</p> <p>Penetrating computer material in order to commit other offense</p> <p>5. If a person committed an act prohibited under section 4, in order to commit an offense under any enactment other than this Law, then he shall be liable to five years imprisonment.</p>		

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>paragraph – foreseeing, as a nearly certain possibility, that the act or the threat will cause fear or panic among the public is equivalent to having a goal to cause fear or panic among the public;</p> <p>(2) the act that was committed or that was planned or the threat included:</p> <p>(a) actual injury to a person’s body or his freedom , or placing a person in danger of death or danger of grievous bodily injury;</p> <p>(b) the creation of actual danger to the health or security of the public;</p> <p>(c) serious damage to property;</p> <p><u>(d) serious disruption of vital infrastructures, systems or services;</u></p> <p>(b) if the aforementioned act or threat was committed or was planned to be committed using weapons as defined in Section 144(c)(1) and (3) of the Penal Law, excluding a weapon part or accessory, it will be considered an act of terrorism even if the conditions of paragraph (1) of subsection (a) are not met, and if it was committed or planned to be committed using chemical, biological or radioactive weapons that are liable, due to their nature, to cause actual</p>	<p>operation, but exclusive of a penetration of computer material which constitutes monitoring under the Secret Monitoring Law 5739-1979.</p> <p>[...]</p> <p>Computer virus</p> <p>6. (a) If a person prepared wrote software in a manner that enables it to disrupt or to cause damage to unspecified computers or computer material, in order to cause unlawful disruption or damage to computers or computer material, either specified or unspecified, then he shall be liable to three years imprisonment.</p> <p>(b) If a person transmitted to another or introduced into another person’s computer software that can cause disruption or damage as said in subsection (a), in order to cause aforesaid unlawful disruption or damage, then he shall be liable to five years imprisonment.</p>			
---	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

mass harm – even if the conditions set forth in paragraphs (1) and (2) of subsection (a) are not met.				
---	--	--	--	--

Source(s): The quoted legislation available at <http://www.justice.gov.il/NR/rdonlyres/4FE9E898-1264-4561-B7AA-0957F6DEA67A/0/ProhibitionTerroristFinancing.doc> and <http://www.cybercrimelaw.net/laws/countries/israel.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

JAPAN

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Penal Code</p> <p>Article 258 Destruction of official electromagnetic records</p> <p>Any person who destroys any documents or electromagnetic record which ought to be used at a State office shall be punished with penal servitude for more than 3 months and not more than 5 years.</p> <p>Unauthorized Computer Access Law</p> <p>Law No. 128 of 1999</p> <p>(Prohibition of acts of unauthorized computer access)</p> <p>Article 3. No person shall conduct an act of unauthorized computer access. 2. The act of unauthorized computer access mentioned in the preceding</p>			<p>Unauthorized Computer Access Law</p> <p>(Prohibition of acts of facilitating unauthorized computer access)</p> <p>Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>paragraph means an act that falls under one of the following items:</p> <p>(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another persons identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);</p> <p>(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);</p> <p>(3) An act of making available a restricted specific use by making in</p>			<p>approval of that access administrator or of that authorized user.</p>
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication, any information or command that can evade the restriction concerned.</p> <p>(Prohibition of acts of facilitating unauthorized computer access) Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.</p> <p>(Penal provisions) Article 8. A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen: (1) A person who has infringed the</p>			
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	provision of Article 3, paragraph 1; Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.			
--	--	--	--	--

Source(s): The quoted legislation available at http://www.isc.meiji.ac.jp/~sumwel_h/Arc-Laws/Penal%20Code%20Japan.htm and <http://www.cybercrimelaw.net/laws/countries/japan.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

KOREA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Criminal Code</p> <p>Article 141 (Invalidity of Public Documents, etc. and Destruction of Public Goods)</p> <p>(1) A person who damages or conceals documents or other goods, or special media records, such as electromagnetic records, etc., used by public offices, or spoils its utility by other methods, shall be punished by imprisonment with prison labor for not more than 7 years or by a fine not exceeding 10 million won.</p> <p>Amended by Act No. 5057, Dec. 29, 1995</p> <p>Article 227-2 (False Preparation or Alteration of Public Electromagnetic Records)</p> <p>A person with the intention of disrupting business falsely or alters electromagnetic documents of public official or public office shall be punished by imprisonment with prison labor not more than 10 years.</p>		<p>Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.</p> <p>Article 65 (Penal Provisions)</p> <p>(1) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 1 year or by a fine not exceeding 10 million won;</p> <p>[...]</p> <p>(4) A person who has repeatedly sent words, sounds, letters, visuals, or films inciting fears and uneasiness to any other person through information and communications networks.</p>	

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>This Article Wholly Amended by Act No. 5057. Dec. 29,1995 Article 232-2 (Falsification or Alteration of Private Electromagnetic Records) A person who falsifies or alters, with the intention of making any error in the management of affairs, any special media records, such as another person's electromagnetic records concerning any years, shall be punished by imprisonment with prison labor for not more than 5 years, or a fine not exceeding 10 million won.</p> <p>This Article Wholly Amended by Act No. 5057. Dec. 29,1995 Article 316 (Violation of Secrecy) (1) A person who opens a sealed or other secretly composed letter, document, or drawing shall be punished by imprisonment with or without labor for not more than 3 years or by a fine not exceeding 5 million won. Amended by Act No. 5057. Dec. 29,1995</p> <p>(2) Any person who detects the contents of another person's sealed or secretly designed letter, document, drawing, picture, or special media records, such as electromagnetic records, using any technical means, shall be subject to the same punishment referred to in paragraph (1).</p> <p>Newly Inserted by Act No. 5057. Dec. 29,1995</p>			
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>Article 347-2 (Fraud by The Use of Computer, etc.) Any person who acquires any benefits to property or has a third person acquire them, by making any data processed after inputting a false information or improper order, or inputting or altering the data without any authority into the data processor, such as computer, etc., shall be punished by imprisonment with prison labor for not more than 10 years, or a fine not exceeding 20 million won. This Article Wholly Amended by Act No. 5057. Dec. 29,1995</p> <p>Article 366 (Destruction and Damage, etc. of Property) A person who, by destroying, damaging, or concealing another's property document or special media records, such as electromagnetic records, etc., or by any other means, reduces their utility, shall be punished by imprisonment with prison labor for not more than 3 years or a fine not exceeding 7 million won. Amended by Act No. 5057. Dec. 29,1995</p> <p>Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. CHAPTER VI Stability of the Information and Communications</p>			
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>Network</p> <p>Article 48 (Prohibition on Act of Infiltrating into Information and Communications Networks, etc.)</p> <p>(1) Any person shall be prohibited from infiltrating into information and communications networks without any justifiable access right or beyond his/her permitted access right.</p> <p>(2) Any person shall be prohibited from transmitting or distributing any program (hereinafter referred to as a "malicious program") that may damage, disrupt, and destroy the information and communications system, alter and forge the data or programs, etc., or hinder the operation thereof without any justifiable reasons.</p> <p>(3) Any person shall be prohibited from sending a large volume of signals or data for the purpose of hindering the stable operation of information and communications networks or from causing troubles in information and communications networks using the method of getting unfair instructions processed.</p> <p>Article 49 (Protection of Secrets, etc.)</p> <p>Any person shall be prohibited from damaging the information of other persons or from infringing, stealing or leaking the secrets of other persons, which are processed, stored or</p>			
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>transmitted by information and communications networks.</p> <p>CHAPTER IX PENAL PROVISIONS</p> <p>Article 61 (Penal Provisions) (1) Any person who has defamed any other person by alleging openly facts through information and communications network with the purpose of slandering him/her shall be punished by imprisonment with or without prison labor for not more than 3 years or by a fine not exceeding 20 million won. (2) Any person who has defamed any other person by alleging openly false facts through information and communications network with the purpose of slandering him/her shall be punished by imprisonment with prison labor for not more than 7 years or the suspension of disqualification for not more than 10 years, or by a fine not exceeding 50 million won.</p> <p>Article 62 (Penal Provision) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 5 years or by a fine not exceeding 50 million won. (1) A person who has utilized the personal information or provided it to any third person beyond the scope of the</p>			
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>notification or the limit specified in a standardized contract under Article 22 (2) in contravention of Article 24 (1) (including a case where the provisions are applied mutatis mutandis in Article 58);</p> <p>(2) A person who has utilized the personal information of users for other purpose than the purpose for which such personal information has been provided or provided such personal information to any other person in contravention of Article 24 (2) (including a case where the provisions are applied mutatis mutandis in Article 58);</p> <p>(3) A person who has damaged, infringed or leaked the personal information of users in contravention of Article 24 (4) (including a case where the provisions are applied mutatis mutandis in Article 58);</p> <p>(4) A person who has transmitted or distributed malicious programs in contravention of Article 48 (2);</p> <p>(5) A person who has caused troubles in information and communications networks in contravention of Article 48 (3); and</p> <p>(6) A person who has damaged the information of any other person, or infringed, stolen or leaked the secrets of any other person in contravention of Article 49.</p>			
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>Article 63 (Penal Provisions) Any person falling under any of the following subparagraphs shall be punished by imprisonment with the prison labor for not more than 3 years or by a fine not exceeding 30 million won; (1) A person who has infiltrated information and communications networks in contravention of Article 48 (1); and (2) A person who has leaked the secrets to any other person, which he/she has learned while performing his duties, or utilized such secrets for other purpose than the purpose of his/her duties in contravention of Article 57.</p> <p>Article 65 (Penal Provisions) (1) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 1 year or by a fine not exceeding 10 million won; [...]</p> <p>(4) A person who has repeatedly sent words, sounds, letters, visuals, or films inciting fears and uneasiness to any other person through information and communications networks.</p>			
--	---	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/korea.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

MOLDOVA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Criminal Code</p> <p>Article 343. Diversion</p> <p>Perpetration of explosions, arsons or some other actions for the purpose of weakening the economics and the defending capacity of the Republic of Moldova, straighten for people’s mass destruction, for causing bodily and health harms to more persons, for distorting and deteriorating of enterprises, buildings, ways of communications, <u>means of telecommunications, or of some other state or public goods</u>, as well as the provocation for the same purpose a different kind of poisons or the spread out of epidemic or bacteria.</p> <p>Is to be punished by imprisonment for the period of sixteen up to twenty-five years or by life imprisonment.</p> <p><i>(Article 278. Terrorism</i></p>	<p>Criminal Code</p> <p>Article 259. Illegal access to the computerized information</p> <p>Illegal access to the computerized information, namely to the information stored in computers, on the material supports of information, on informational system or network, if this access is accompanied by deterioration, modification, shutting of, or copying of the information, or by disturbing the work of computers, of system or of computer’s network,-</p> <p>Shall be punished with a fine in amount of 200 to 500 conventional units or with imprisonment for a period of up to 2 years.</p> <p>Article 260. Introduction or spreading of virus programs</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p><i>(1) Terrorism, meaning provoking explosions, setting on fire or other actions that endanger human lives or cause material damage on a large scale or other serious consequences, when these acts were committed with the purpose of violating public safety, intimidation of the population or in order to force the public authorities or physical persons to take certain decisions, or threatening to commit such acts in these purposes,</i></p> <p><i>Shall be punished by jail sentence of between 5 and 10 years.</i></p> <p><i>(2) The same acts, when committed:</i></p> <p><i>a) repeatedly;</i></p> <p><i>b) by an organized criminal group;</i></p> <p><i>c) by use of firearms or explosive;</i></p> <p><i>d) causing gross or medium bodily or health harm;</i></p> <p><i>e) causing material damage in especially large proportions,</i></p> <p><i>Shall be punished by jail sentence of between 8 and 15 years.</i></p> <p><i>(3) Acts set forth in paragraphs (1) or (2):</i></p>	<p>(1) Knowingly introducing into the computer programs of modifications with a virus character or spreading of computer programs that deteriorate the material supports of information, data processing equipment or violates the protection system,</p> <p>Shall be punished by a fine in the amount of 300 to 800 conventional units or by jail sentence of between 2 and 5 years.</p> <p>(2) Spreading of virus programs for computers that caused serious consequences,</p> <p>Shall be punished by jail sentence of between 4 and 8 years.</p> <p>[...]</p> <p>Article 343. Diversion</p> <p>Perpetration of explosions, arsons or some other actions for the purpose of weakening the economics and the defending capacity of the Republic of Moldova, straighten for people’s mass destruction, for causing bodily and health harms to more persons, for distorting and deteriorating of enterprises, buildings, ways of communications, means of telecommunications, or of some other state or public goods, as well as the</p>			
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p><i>a) committed by a criminal organization;</i></p> <p><i>b) that caused death of the person by negligence;</i></p> <p><i>Shall be punished by jail sentence of between 12 and 20 years.</i></p> <p><i>(4) Terrorism associated with intended murder,</i></p> <p><i>Shall be punished by jail sentence of between 16 and 25 years or by detention for life.</i></p> <p><i>(5) The person, who committed the terrorist act or other co-participants can be punished by minimal sentences provided by the present article, in case they warned the public authorities about the acts and thus contributed to avoiding death of the person or causing bodily or health harm or other serious consequences, or exposed other participants.</i></p> <p><i>(6) Person who participated at the preparation of the terrorist act is exempted of the criminal liability if he announced on time the public authorities or by any other means prevented committing of terrorist act and if the acts of this person do not include other crime components.)</i></p>	<p>provocation for the same purpose a different kind of poisons or the spread out of epidemic or bacteria.</p> <p>Is to be punished by imprisonment for the period of sixteen up to twenty-five years or by life imprisonment.</p>			
---	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

NORWAY

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Penal Code</p> <p>§ 151 b: Any person who by destroying, damaging, or putting out of action any data collection or any installation for supplying power, broadcasting, telecommunication, or transport causes comprehensive disturbance in the public administration or in community life in general shall be liable to imprisonment for a term not exceeding 10 years. Negligent acts of the kind mentioned in the first paragraph shall be punishable by fines or imprisonment for a term not exceeding one year. Accomplices shall be liable to the same penalty.</p>			<p>Penal Code</p> <p>§145b: Any person who unlawfully makes available a computer password or similar data, by which the whole or any part of a computer system is capable of being accessed, shall be sentenced for spreading of access data, to a fine or imprisonment not exceeding 6 months or both. Serious spreading of access data shall be sentenced to imprisonment not exceeding 2 years. In deciding whether the spreading is serious, special regard shall be paid to whether the data may access sensitive information, whether the spreading is extensive or whether the conduct in other respects</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

				causes a danger for considerable damage. An accomplice shall be liable to the same penalty.
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/norway.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

POLAND

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Criminal Code</p> <p>Article 267. § 1. Whoever, without being authorized to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.</p> <p>§ 2. The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorized to access, installs or uses tapping, visual detection or other special equipment.</p> <p>§ 3. The same punishment shall be imposed on anyone, who imparts to another person the information obtained in the manner specified in § 1 or 2 discloses to another person.</p> <p>§ 4. The prosecution of the offence</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>specified in §1 – 3 shall occur on a motion of the injured person.</p> <p>Article 268. § 1. Whoever, not being himself authorized to do so, destroys, damages, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorized person to obtain knowledge of that information, shall be subject to a fine, the penalty of liberty or the penalty of deprivation of liberty for up to 2 years.</p> <p>§ 2. If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.</p> <p>§ 3. Whoever, by committing an act specified in § 1 or 2, causes a significant loss of property shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.</p> <p>§ 4. The prosecution of the offence specified in § 1-3 shall occur on a motion of the injured person.</p> <p>Article 269. §1. <u>Whoever destroys, deletes or changes a record on an electronic information carrier, having a particular significance for national defense, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic</u></p>			
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p><u>collection and transmission of such information</u>, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years. § 2. The same punishment shall be imposed on anyone, who commits the act specified in §1 by damaging a device used for the automatic processing, collection or transmission of information.</p>			
--	---	--	--	--

Source(s): The quoted legislation available at <http://www.cybercrimelaw.net/laws/countries/poland.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

ROMANIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Criminal Code</p> <p>Terrorist acts</p> <p>Art.295 – (1) The following offences are terrorist acts when they are committed in order to seriously disturb public order, through intimidation, terror or by creating a state of panic:</p> <p>a) offences of homicide and first degree homicide provided in Art.178 and Art.179, corporal injury and serious corporal injury provided in Art.186 and 187, as well as illegal deprivation of freedom provided in Art.201;</p> <p>b) the offences provided in Art.105-108 of the Aerial Code;</p> <p>c) offences of destruction in Art.263 and 264;</p> <p>d) offences of non-abidance by the legal</p>	<p>Anti-corruption law Title III on preventing and fighting cyber-crime</p> <p>Section 1 Offences against the confidentiality and integrity of data and computer systems</p> <p>Art.42 – (1) The illegal access to a computer system is a crime and is punished with imprisonment from 6 months to 3 years.</p> <p>(2) If the fact mentioned at item (1) is performed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.</p> <p>Art.43 – (1) The illegal interception of any transmission of computer data that is not published to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.</p> <p>(2) The same punishment is applied also for the illegal interception, of electromagnetic emissions from a</p>			<p>Anti-corruption law Title III on preventing and fighting cyber-crime</p> <p>Art.46 – (1) The following are considered criminal offences and punished with imprisonment from one to 6 years.</p> <p>a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer programme designed or adapted fro the purpose of committing one of the offences established in accordance with arts.42-45;</p> <p>b) the production, sale, import, distribution or making available, in any other form, without right, of</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>treatment of weapons and ammunition, non-observance of the legal treatment of nuclear material and other radioactive materials, as well as non-compliance with the legal treatment of explosives, provided in Art.406-408;</p> <p>e) the act of inserting or spreading, into the atmosphere, on the soil, into the underground or in water, products, substances, materials, microorganisms or toxins likely to endanger the health of people or animals or the environment;</p> <p>f) threats with bombs or other explosives.</p> <p>(2) For the offences in para.(1) a)-d) the special maximum of the penalty provided in the law shall be applied, which can be increased up to its general maximum, and if the general maximum is not sufficient, the penalty can be increased up to the general maximum of the immediately superior penalty.</p> <p>(3) For the offence in para.(1) e), the penalty shall be severe detention from 15 to 20 years and the prohibition of certain rights, and for the offence in para.(1) f), the penalty shall be strict imprisonment from 3 to 10 years and the prohibition of certain rights.</p> <p>(4) Attempt shall be sanctioned by the penalty provided for the offence when it</p>	<p>computer system carrying non-public computer data.</p> <p>Art.44 – (1) The illegal alteration, deletion or deterioration of computer data of the access restriction to such data is considered a criminal offence and is punished with imprisonment from 2 to 7 years.</p> <p>(2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years.</p> <p>(3) The unauthorised data transfer by means of an information data storing mean is also punish as in paragraph (2).</p> <p>Art.45 – The serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to these data is considered a criminal offence and is punished with imprisonment from 3 to 15 years.</p> <p>[...]</p> <p>Section 2</p> <p>Computer-related offences</p> <p>Art.48. – The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to these data, resulting in inauthentic data, with the intent to be used for legal purposes, is considered a criminal</p>			<p>a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of one of the offences established in accordance with arts.42-45;</p> <p>(2) The possession, without right, of a device, computer programme, password, access code or computer data referred to at paragraph (1) for the purpose of one of the offences established in accordance with arts.942-45 is also punished similarly.</p>
--	---	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>takes place or by a penalty within the immediately inferior limits of the penalty provided in the law for the offence when it takes place.</p> <p>(5) The act of producing or obtaining the means or the instruments, as well as of taking measures in order to commit the offences in para. (1) shall also be considered attempt.</p> <p>(6) Agreement in order to commit terrorist acts shall be punished by strict imprisonment from 3 to 15 years and the prohibition of certain rights.</p>	<p>offence and is punished with imprisonment from 2 to 7 years.</p> <p>Art.49 – Causing the loss of property to a person by the input, alteration or deletion of computer data, by restricting the access to such data or by preventing in any way the operation of a computer system, in order to obtain an economic benefit for oneself or for another is punished with imprisonment from 3 to 12 years.</p> <p>Art.50 – The intent to commit the offences referred to in arts.48 and 49 is also punished.</p>			
---	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org> and <http://www.cybercrimelaw.net/laws/countries/romania.html>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

RUSSIAN FEDERATION

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
	<p>Criminal Code</p> <p>Article 272. Unauthorized access to computer information</p> <p>1. Unauthorized access to law protected computer information in the electronic computers, their systems or networks or on the machine carriers resulted in erasing, blocking or copying computer information, disturbing the work of electronic computers, their systems or networks is punished with fine from two hundred to five hundred minimum wages, condemned person’s wages or another income within the term from two to five months, refinery works within the term from six months to one year, or imprisonment within up to two years.</p> <p>2. The same action carried out by a group of persons in prior agreement or an organized group or a person abusing his official position and having equally an access to electronic computers, their systems or networks is punished with fine</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>from five hundred to eight hundred minimum wages, condemned person’s wages or another income within the term from five to eight months, refinery works within the term from one to two years, arrest within the term from three to six months or imprisonment within up to five years.</p> <p>Article 273. Production, use and spread of detrimental electronic computer programs</p> <p>1. Production of electronic computer programs or introduction of changes into current programs resulted in erasing, blocking, modifying or copying information, disturbing the work of electronic computers, their systems or networks and use or spread of these programs are punished with imprisonment within up to three years with fine from two hundred to five hundred minimum wages or condemned person’s wages or another income within the term from two to five months.</p> <p>2. The same actions entailed serious consequences through imprudence are punished with imprisonment within the term from three to seven years.</p> <p>Article 274. Violation of electronic computer, system or network operating rules</p> <p>1. Violation of electronic computer, system or network operating rules on the part of a person having an access to</p>			
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	electronic computers, their systems or networks resulted in erasing, blocking or modifying law protected information and caused a considerable damage is punished with denial of particular position or activity privileges within up to five years, obligatory works within the term from one hundred and eighty to two hundred hours or freedom limitation within up to two years.			
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

SERBIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Criminal Code</p> <p>Malicious Destruction</p> <p>Article 313</p> <p>Whoever with intent to undermine the constitutional order or security of Serbia or SaM by demolishing, setting fire or otherwise destroying or damaging industrial, agricultural <u>or other economic facility, communications equipment,</u> public utility equipment for water, heating, gas or power supply, a dam, warehouse, building <u>or other structure of importance for security or supply of citizens or to the economy or functioning of public services,</u> shall be punished by imprisonment of three to fifteen years.</p>	<p>Criminal Code</p> <p>Destroying and Damaging Public Infrastructure</p> <p>Article 279</p> <p>(1) Whoever destroys, damages, alters or makes useless or removes public infrastructure equipment for water, heating, gas, electrical or other power supply <u>or communications system equipment and thereby causes disruption in life of citizens or in functioning of the economy,</u> shall be punished by imprisonment of three months to five years.</p> <p>(2) Whoever commits the offence specified in paragraph 1 of this Article from negligence, shall be punished by fine or imprisonment up to one year.</p>	<p>Criminal Code</p> <p>Computer Fraud</p> <p>Article 301</p> <p>(1) Whoever enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data with intent to acquire for himself or another unlawful material gain and thus causes material damage to another person, shall be punished by fine or imprisonment up to three years.</p> <p>(2) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding four hundred</p>		<p>Criminal Code</p> <p>Unauthorized Access to Computer, Computer Network or Electronic Data Processing</p> <p>Article 302</p> <p>(1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorization, or accesses electronic data processing without authorization, shall be punished by fine or imprisonment up to six months.</p> <p>(2) Whoever uses data obtained in manner provided under paragraph 1 of this</p>

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p><i>(Terrorism</i></p> <p><i>Article 312</i></p> <p><i>Whoever with intent to compromise the constitutional order or security of Serbia or SaM causes an explosion or fire or commits another generally dangerous act or commits an abduction of a person or some other act of violence, or by threat of committing such generally dangerous act or use of nuclear, chemical, bacteriological or other dangerous substance and thereby causes fear or insecurity among citizens, shall be punished by imprisonment of three to fifteen years.)</i></p>	<p>[...]</p> <p>Damaging Computer Data and Programs</p> <p>Article 298</p> <p>(1) Whoever without authorization deletes, alters, damages, conceals or otherwise makes unusable a computer datum or program, shall be punished by fine or imprisonment up to one year.</p> <p>(2) If the offence specified in paragraph 1 of this Article results in damages exceeding four hundred and fifty thousand dinars, the offender shall be punished by imprisonment of three months to three years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in damages exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of three months to five years.</p> <p>(4) Equipment and devices used in perpetration of the offence specified in paragraphs 1 and 2 of this Article shall be seized.</p> <p>Computer Sabotage</p>	<p>and fifty hundred thousand dinars, the offender shall be punished by imprisonment of one to eight years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in acquiring material gain exceeding one million five hundred thousand dinars, the offender shall be punished by imprisonment of two to ten years.</p> <p>(4) Whoever commits the offence specified in paragraph 1 of this Article from malicious mischief, shall be punished by fine or imprisonment up to six months.</p> <p>[...]</p> <p>Unauthorized Use of Computer or Computer Network</p> <p>Article 304</p> <p>(1) Whoever uses computer services or computer network with intent to acquire unlawful material gain for himself or another, shall be punished by fine or imprisonment up to</p>		<p>Article, shall be punished by fine or imprisonment up to two years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted, the offender shall be punished by imprisonment up to three years.</p> <p><i>(Revealing of Official Secret</i></p> <p><i>Article 369</i></p> <p><i>(1) An official who without authorization communicates, conveys or otherwise makes available information representing an official secret or whoever obtains such information with intent to convey it to an unauthorized person, shall be punished by imprisonment of three months to five years.</i></p>
--	---	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>Article 299</p> <p>98</p> <p>Whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer datum or program or damages or destroys a computer or other equipment for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, enterprises or other entities, shall be punished by imprisonment of six months to five years.</p> <p>Creating and Introducing of Computer Viruses</p> <p>Article 300</p> <p>(1) Whoever makes a computer virus with intent to introduce it into another’s computer or computer network, shall be punished by fine or imprisonment up to six months.</p> <p>(2) Whoever introduces a computer virus into another’s computer or computer network thereby causing damage, shall be punished by fine or imprisonment up to two years.</p>	<p>three months.</p> <p>(2) Prosecution for the offence specified in paragraph 1 of this Article shall be instigated by private action.</p>	<p><i>(2) If the offence specified in paragraph 1 of this Article is committed for gain or in respect of particularly confidential information or for publishing or use abroad, the offender shall be punished by imprisonment of one to eight years.</i></p> <p><i>(3) If the offence specified in paragraph 1 of this Article is committed from negligence, the offender shall be punished by imprisonment up to three years.</i></p> <p><i>(4) An official secret is information and documents declared by law, other regulation or decision of the competent authority issued pursuant to law as an official secret and whose disclosure would cause or could cause damage to the service.</i></p> <p><i>(5) Data and documents directed at serious violation of fundamental rights of man, or at endangering the constitutional order and security of Serbia and SaM, as well as data and</i></p>
--	---	---	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>(3) Equipment and devices used for committing of the offence specified in paragraphs 1 and 2 of this Article shall be seized.</p> <p>[...]</p> <p>Unauthorized Access to Computer, Computer Network or Electronic Data Processing</p> <p>Article 302</p> <p>(1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorization, or accesses electronic data processing without authorization, shall be punished by fine or imprisonment up to six months.</p> <p>(2) Whoever uses data obtained in manner provided under paragraph 1 of this Article, shall be punished by fine or imprisonment up to two years.</p> <p>(3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted, the offender shall be punished by imprisonment up to three</p>			<p><i>documents that have as objective concealing of a committed criminal offence punishable under law by imprisonment of five or more years shall not be deemed an official secret in terms of paragraph 4 of this Article.</i></p> <p><i>(6) Provisions specified in paragraphs 1 through 4 of this Article shall also be applied to a person who has disclosed an official secret after his position of an official has ceased.)</i></p>
--	---	--	--	---

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>years.</p> <p>Preventing or Restricting Access to Public Computer Network</p> <p>Article 303</p> <p>(1) Whoever without authorization prevents or hinders access to a public computer network, shall be punished by fine or imprisonment up to one year.</p> <p>(2) If the offence specified in paragraph 1 of this Article is committed by an official in discharge of duty, such official shall be punished by imprisonment up to three years.</p>			
--	---	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

SLOVAKIA

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Criminal Code</p> <p>Section 94</p> <p>Terrorism</p> <p>(1) Any person who, with the intention to seriously intimidate the population, to seriously destabilize or destroy the constitutional, political, economic or social order of the country or of an international organization or to force a government of a country or an international organization to do something or to refrain from doing something, threatens to commit or has intentionally committed an particularly serious crime (Section 41 paragraph 2) imperilling the life, health of people or property shall be liable to a term of imprisonment of twelve to fifteen years or to an exceptional sentence of imprisonment or confiscation of property.</p> <p>(2) The offender shall be liable to an</p>	<p>Criminal Code</p> <p>Section 257a Damaging or Misusing Data Carrier Record</p> <p>(1) A person, who with intent to cause damage or some other detriment to another or obtain unjust benefit for himself or another person, gains access to a data carrier and:</p> <p>(a) uses such data without authorization;</p> <p>(b) destroys, damages or renders useless the data on such carrier;</p> <p>(c) interferes with the hardware or software of a particular computer,</p> <p>shall be punished by a term of imprisonment of from six months to three years, by prohibition of a specific activity, by a pecuniary penalty or</p>		<p><i>Proposed amendment to the Criminal Code to include criminalization of distribution or publication through a computer system of material which denies, grossly minimizes, approves or justifies the criminal acts of genocide or crimes against humanity to be punished by a fine or prison term of 3 months – 3 years (obligation referred to in §6 of the Additional Protocol to the Convention on Cybercrime.</i></p>	

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>exceptional sentence of imprisonment and confiscation of property if</p> <p>a)he commits the offence referred to in paragraph 1 as a member of a terrorist group,</p> <p>b)he commits such an offence in a particularly brutal manner,</p> <p>c)he causes through the commission of such an offence serious bodily harm or death of several persons,</p> <p>d)he commits such an offence against constitutional officials, persons protected by international law, armed forces, armed security corps or armed corps.</p>	<p>forfeiture of a specific thing.</p> <p>(2) An offender shall be sentenced to a term of imprisonment of from one year to five years if:</p> <p>a) he commits an act under subsection (1) as a member of an organized group, or</p> <p>b) by such act he causes substantial damage or acquires substantial benefit for himself or another person.</p> <p>(3) An offender shall be sentenced to a term or imprisonment of from two years to eight years if, by an act under subsection (1), he causes large-scale damage or acquires a large-scale benefit for himself or another person.</p>			
--	---	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

UKRAINE

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Law on Combating Terrorism</p> <p>Article 1. Determination of basic terms</p> <p>In this Law the stated terms below are used in such value:</p> <p>terrorism - publicly dangerous activity, which consists in conscious, purposeful application of violence by the capture of hostages, arsons, murders, tortures, intimidation of population and organs of power or accomplishing of other encroachments on the life or health of in anything not guilty people or threats of accomplishing of criminal acts with the purpose of achievement of criminal purposes;</p> <p>[...]</p> <p>technological terrorism is the crimes, which are accomplished with a terrorist purpose with application of nuclear, chemical, bacteriological (biological) and other weapon</p>	<p>Criminal Code</p> <p>Article 361 (illegal interference with computers, computer systems and networks)</p> <p>1. Illegal intrusion into computer systems, networks, resulting in deletion or damaging of information contained therein, or information carriers; spreading of computer viruses results in either penalty ranging up to 70 minimal wages, or deprivation of liberty or penitential labour up to two years.</p> <p>2. Same actions resulting in serious damage, or conducted repeatedly, or upon previous arrangement by group of persons results in restriction of liberty up to three years or deprivation of liberty from three to five years.</p>			

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>of mass defeat or its components, other matters insalubrious people, and <u>facilities of electromagnetic action, computer systems and of communication networks</u>, including fascination, lay-up and destruction potentially of dangerous objects, which straight or mediated created or threaten by the origin of threat of extraordinary situation as a result of these actions and make a danger for a personnel, population and environment; terms are created for failures and industrial disasters.</p>				
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

UNITED KINGDOM

Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT	Measures against the use of computers and/or computer networks as tools and/or targets	Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)	Use of the Internet and electronic media in disseminating terrorist messages, including propaganda	Regulation of the use of cryptography
<p>Terrorism Act 2000</p> <p>1.—(1) In this Act “terrorism” means the use or threat of action Terrorism:</p> <p>interpretation. where—</p> <p>(a) the action falls within subsection (2),</p> <p>(b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and</p> <p>(c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.</p> <p>(2) Action falls within this subsection if it—</p> <p>(a) involves serious violence against a person,</p> <p>(b) involves serious damage to property,</p>	<p>Terrorism Act 2000</p> <p>Schedule 9</p> <p>Scheduled Offences</p> <p>[...]</p> <p>Computer Misuse Act 1990 (c. 18)</p> <p>19. Offences under the following provisions of the Computer Misuse Act 1990 subject to note 1 below—</p> <p>(a) section 1 (unauthorised access to computer material),</p> <p>(b) section 2 (unauthorised access with intent to commit further offence), and</p> <p>(c) section 3 (unauthorised modification).</p>	<p>Terrorism Act 2000</p> <p>58.—(1) A person commits an offence if— Collection of information. (a) he collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or</p> <p>(b) he possesses a document or record containing information of that kind.</p> <p><u>(2) In this section “record” includes a photographic or electronic record.</u></p> <p>[...]</p> <p>103.—(1) A person commits an offence if— Terrorist</p>	<p>Terrorism Act 2006</p> <p>2. Dissemination of terrorist publications</p> <p>(1) A person commits an offence if he engages in conduct falling within subsection (2) and, at the time he does so-</p> <p>(a) he intends an effect of his conduct to be a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism;</p> <p>(b) he intends an effect of his conduct to be the provision of assistance in the commission or preparation of such acts; or</p> <p>(c) he is reckless as to whether his conduct has an effect mentioned in paragraph (a) or</p>	

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>(c) endangers a person’s life, other than that of the person committing the action,</p> <p>(d) creates a serious risk to the health or safety of the public or a section of the public, or</p> <p>(e) <u>is designed seriously to interfere with or seriously to disrupt an electronic system.</u></p>	<p>Computer Misuse Act 1990</p> <p>Computer misuse offences</p> <p>Unauthorised access to computer material.</p> <p>1.—(1) A person is guilty of an offence if—</p> <p>(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;</p> <p>(b) the access he intends to secure is unauthorised; and</p> <p>(c) he knows at the time when he causes the computer to perform the function that that is the case.</p> <p>(2) The intent a person has to have to commit an offence under this section need not be directed at—</p> <p>(a) any particular program or data;</p> <p>(b) a program or data of any particular kind; or</p> <p>(c) a program or data held in any particular computer.</p> <p>(3) A person guilty of an offence under</p>	<p>information. (a) he collects, makes a record of, publishes, communicates or attempts to elicit information about a person to whom this section applies which is of a kind likely to be useful to a person committing or preparing an act of terrorism, or</p> <p>(b) he possesses a document or record containing information of that kind.</p> <p>(2) This section applies to a person who is or has been—</p> <p>(a) a constable,</p> <p>(b) a member of Her Majesty’s Forces,</p> <p>(c) the holder of a judicial office,</p> <p>(d) an officer of any court, or</p> <p>(e) a full-time employee of the prison service in Northern Ireland.</p> <p><u>(3) In this section “record” includes a photographic or</u></p>	<p>(b).</p> <p>(2) For the purposes of this section a person engages in conduct falling within this subsection if he- [...] <u>(e) transmits the contents of such a publication electronically.</u></p> <p>[...]</p> <p>3. Application of ss. 1 and 2 to internet activity etc.</p> <p>(1) This section applies for the purposes of sections 1 and 2 in relation to cases where- <u>(a) a statement is published or caused to be published in the course of, or in connection with, the provision or use of a service provided electronically; or</u></p> <p><u>(b) conduct falling within section 2(2) was in the course of, or in connection with, the provision or use of such a service.</u></p> <p>(2) The cases in which the statement, or the article or record to which the conduct relates, is to be regarded as having the endorsement of a</p>	
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.</p> <p>Unauthorised access with intent to commit or facilitate commission of further offences.</p> <p>2.—(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—</p> <p>(a) to commit an offence to which this section applies; or</p> <p>(b) to facilitate the commission of such an offence (whether by himself or by any other person);</p> <p>and the offence he intends to commit or facilitate is referred to below in this section as the further offence.</p> <p>(2) This section applies to offences—</p> <p>(a) for which the sentence is fixed by law; or</p> <p>(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or,</p>	<p><u>electronic record.</u></p> <p>Computer Misuse Act 1990</p> <p>Computer misuse offences</p> <p>[...]</p> <p>Unauthorised access with intent to commit or facilitate commission of further offences.</p> <p>2.—(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—</p> <p>(a) to commit an offence to which this section applies; or</p> <p>(b) to facilitate the commission of such an offence (whether by himself or by any other person);</p> <p>and the offence he intends to commit or facilitate is referred to below in this section as the further offence.</p> <p>(2) This section applies to</p>	<p>person ("the relevant person") at any time include a case in which-</p> <p>(a) a constable has given him a notice under subsection (3);</p> <p>(b) that time falls more than 2 working days after the day on which the notice was given; and</p> <p>(c) the relevant person has failed, without reasonable excuse, to comply with the notice.</p> <p>(3) A notice under this subsection is a notice which-</p> <p>(a) declares that, in the opinion of the constable giving it, the statement or the article or record is unlawfully terrorism-related;</p> <p>(b) requires the relevant person to secure that the statement or the article or record, so far as it is so related, is not available to the public or is modified so as no longer to be so related;</p> <p>(c) warns the relevant person that a failure to comply with the notice within 2 working</p>	
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).</p> <p>(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.</p> <p>(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.</p> <p>(5) A person guilty of an offence under this section shall be liable—</p> <p>(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and</p> <p>(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.</p> <p>Unauthorised modification of computer material.</p> <p>3.—(1) A person is guilty of an offence if—</p> <p>(a) he does any act which causes an unauthorised modification of the contents</p>	<p>offences—</p> <p>(a) for which the sentence is fixed by law; or</p> <p>(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).</p> <p>(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.</p> <p>(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.</p> <p>(5) A person guilty of an offence under this section shall be liable—</p> <p>(a) on summary conviction, to imprisonment for a term not</p>	<p>days will result in the statement, or the article or record, being regarded as having his endorsement; and</p> <p>(d) explains how, under subsection (4), he may become liable by virtue of the notice if the statement, or the article or record, becomes available to the public after he has complied with the notice.</p> <p>(4) Where-</p> <p>(a) a notice under subsection (3) has been given to the relevant person in respect of a statement, or an article or record, and he has complied with it, but</p> <p>(b) he subsequently publishes or causes to be published a statement which is, or is for all practical purposes, the same or to the same effect as the statement to which the notice related, or to matter contained in the article or record to which it related, (a "repeat statement");</p> <p>the requirements of subsection (2)(a) to (c) shall be regarded</p>	
--	--	---	---	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>of any computer; and</p> <p>(b) at the time when he does the act he has the requisite intent and the requisite knowledge.</p> <p>(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—</p> <p>(a) to impair the operation of any computer;</p> <p>(b) to prevent or hinder access to any program or data held in any computer; or</p> <p>(c) to impair the operation of any such program or the reliability of any such data.</p> <p>(3) The intent need not be directed at—</p> <p>(a) any particular computer;</p> <p>(b) any particular program or data or a program or data of any particular kind; or</p> <p>(c) any particular modification or a modification of any particular kind.</p> <p>4) For the purposes of subsection (1)(b) above the requisite knowledge is</p>	<p>exceeding six months or to a fine not exceeding the statutory maximum or to both; and</p> <p>(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.</p>	<p>as satisfied in the case of the repeat statement in relation to the times of its subsequent publication by the relevant person.</p> <p>(5) In proceedings against a person for an offence under section 1 or 2 the requirements of subsection (2)(a) to (c) are not, in his case, to be regarded as satisfied in relation to any time by virtue of subsection (4) if he shows that he-</p> <p>(a) has, before that time, taken every step he reasonably could to prevent a repeat statement from becoming available to the public and to ascertain whether it does; and</p> <p>(b) was, at that time, a person to whom subsection (6) applied.</p> <p>(6) This subsection applies to a person at any time when he-</p> <p>(a) is not aware of the publication of the repeat statement; or</p> <p>(b) having become aware of its publication, has taken every step that he reasonably could to secure that it either ceased to be</p>	
--	--	---	---	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>knowledge that any modification he intends to cause is unauthorised.</p> <p>(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary. (6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.</p> <p>(7) A person guilty of an offence under this section shall be liable—</p> <p>(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and</p> <p>(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.</p>		<p>available to the public or was modified as mentioned in subsection (3)(b).</p> <p>(7) For the purposes of this section a statement or an article or record is unlawfully terrorism-related if it constitutes, or if matter contained in the article or record constitutes-</p> <p>(a) something that is likely to be understood, by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism or Convention offences; or</p> <p>(b) information which-</p> <p>(i) is likely to be useful to any one or more of those persons in the commission or preparation of such acts; and</p> <p>(ii) is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the</p>	
--	--	--	---	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

			<p>purpose of being so useful.</p> <p>(8) The reference in subsection (7) to something that is likely to be understood as an indirect encouragement to the commission or preparation of acts of terrorism or Convention offences includes anything which is likely to be understood as-</p> <p>(a) the glorification of the commission or preparation (whether in the past, in the future or generally) of such acts or such offences; and</p> <p>(b) a suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.</p>	
--	--	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>, <http://www.opsi.gov.uk/Acts/acts2000/20000011.htm> and <http://www.opsi.gov.uk/acts/acts2006/20060011.htm>.

UNITED STATES

<p>Definition of terrorism (and/or related offenses), mention of the link with the Internet and/or the IT</p>	<p>Measures against the use of computers and/or computer networks as tools and/or targets</p>	<p>Use of the IT as support for (physical) terrorist operations (communication, financing, intelligence collection etc.)</p>	<p>Use of the Internet and electronic media in disseminating terrorist messages, including propaganda</p>	<p>Regulation of the use of cryptography</p>
<p>USA PATRIOT Act</p> <p>SEC. 808. DEFINITION OF FEDERAL CRIME OF TERRORISM.</p> <p>Section 2332b of title 18, United States Code, is amended--</p> <p>[...]</p> <p>(2) in subsection (g)(5)(B), by striking clauses (i) through (iii) and inserting the following:</p> <p>“(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 229 (relating to chemical weapons), subsection (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (relating to nuclear</p>	<p>USA PATRIOT Act</p> <p>SEC. 814. DETERRENCE AND PREVENTION OF CYBERTERRORISM.</p> <p>(a) CLARIFICATION OF PROTECTION OF PROTECTED COMPUTERS- Section 1030(a)(5) of title 18, United States Code, is amended--</p> <p>(1) by inserting ‘(i)’ after ‘(A)’;</p> <p>(2) by redesignating subparagraphs (B) and (C) as clauses (ii) and (iii), respectively;</p> <p>(3) by adding ‘and’ at the end of clause (iii), as so redesignated; and</p> <p>(4) by adding at the end the following:</p> <p>“(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused</p>	<p>The Computer Fraud and Abuse Act</p> <p>§ 1030. Fraud and related activity in connection with computers</p> <p>(a) Whoever—</p> <p>(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of</p>		

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>materials), 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), <u>1030(a)(1) (relating to protection of computers), 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v) (relating to protection of computers), 1114</u> (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), <u>1362 (relating to destruction of communication lines, stations, or systems), 1363</u> (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to wrecking trains), 1993 (relating to terrorist attacks and other acts of violence against mass transportation systems), 2155 (relating to destruction of national defense materials, premises, or utilities), 2280 (relating to</p>	<p>(or, in the case of an attempted offense, would, if completed, have caused)--</p> <p>“(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;</p> <p>“(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;</p> <p>“(iii) physical injury to any person;</p> <p>“(iv) a threat to public health or safety; or</p> <p>“(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;’.</p> <p>(b) PROTECTION FROM EXTORTION- Section 1030(a)(7) of title 18, United States Code, is amended by striking ‘, firm, association, educational institution, financial institution,</p>	<p>the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;</p> <p>(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—</p> <p>(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681</p>		
--	---	---	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

<p>violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), or 2340A (relating to torture) of this title.</p>	<p>government entity, or other legal entity,'. (c) PENALTIES- Section 1030(c) of title 18, United States Code, is amended-- (1) in paragraph (2)-- (A) in subparagraph (A) -- (i) by inserting `except as provided in subparagraph (B),' before `a fine'; (ii) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and (iii) by striking `and' at the end; (B) in subparagraph (B), by inserting `or an attempt to commit an offense punishable under this subparagraph,' after `subsection (a)(2),' in the matter preceding clause (i); and (C) in subparagraph (C), by striking `and' at the end; (2) in paragraph (3)-- (A) by striking `, (a)(5)(A), (a)(5)(B),' both places it appears; and (B) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and</p>	<p>et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer if the conduct involved an interstate or foreign communication; (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States; (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers</p>		
---	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>(3) by adding at the end the following:</p> <p>`(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;</p> <p>`(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;</p> <p>`(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.'</p> <p>(d) DEFINITIONS- Section 1030(e) of title 18, United States Code is amended--</p> <p>(1) in paragraph (2)(B), by inserting `, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States' before the semicolon;</p>	<p>the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;</p> <p>(5)</p> <p>(A)</p> <p>(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;</p> <p>(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or</p> <p>(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;</p> <p>and</p>		
--	---	---	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>(2) in paragraph (7), by striking `and' at the end;</p> <p>(3) by striking paragraph (8) and inserting the following:</p> <p>`(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information;';</p> <p>(4) in paragraph (9), by striking the period at the end and inserting a semicolon; and</p> <p>(5) by adding at the end the following:</p> <p>`(10) the term `conviction' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;</p> <p>`(11) the term `loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of</p>	<p>(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—</p> <p>(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;</p> <p>(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;</p> <p>(iii) physical injury to any person;</p> <p>(iv) a threat to public health or safety; or</p> <p>(v) damage affecting a computer system used by or for</p>		
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>service; and</p> <p>`(12) the term `person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.'</p> <p>The Computer Fraud and Abuse Act</p> <p>§ 1030. Fraud and related activity in connection with computers</p> <p>(a) Whoever—</p> <p>(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate,</p>	<p>a government entity in furtherance of the administration of justice, national defense, or national security;</p> <p>(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—</p> <p>(A) such trafficking affects interstate or foreign commerce; or</p> <p>(B) such computer is used by or for the Government of the United States; [1]</p> <p>(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;</p> <p>shall be punished as provided in subsection (c) of this section.</p>		
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;</p> <p>(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—</p> <p>(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);</p> <p>(B) information from any department or agency of the United States; or</p> <p>(C) information from any protected computer if the conduct involved an interstate or foreign communication;</p> <p>(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the</p>			
--	--	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;</p> <p>(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;</p> <p>(5)</p> <p>(A)</p> <p>(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;</p> <p>(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or</p>			
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and</p> <p>(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—</p> <p>(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;</p> <p>(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;</p> <p>(iii) physical injury to any person;</p> <p>(iv) a threat to public health or safety; or</p> <p>(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national</p>			
--	---	--	--	--

*OSCE/ODIHR Comments on Legislative Treatment of “Cyberterror”
in Domestic Law of Individual States*

	<p>security;</p> <p>(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—</p> <p>(A) such trafficking affects interstate or foreign commerce; or</p> <p>(B) such computer is used by or for the Government of the United States; [1]</p> <p>(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;</p> <p>shall be punished as provided in subsection (c) of this section.</p>			
--	---	--	--	--

Source(s): The quoted legislation available at <http://www.legislationline.org>.