The International Cyber Terrorism Regulation Project (ICTRP)
www.ictrp.org

Full Annexes of the Policy Paper

TABLE OF CONTENTS

Annex 1: Taxonomy of Terrorist Use of the Internet

1. Propaganda

The internet facilitates the dissemination of terrorist messages. The use of propaganda is the most fundamental stage in which terrorist organizations spread their ideologies, beliefs and motivations. According to the 2012 United Nations Office on Drugs and Crime (UNODC) report on "The use of the Internet for terrorist purposes" (herein, "the UNODC Report"), propaganda can take the form of "virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers." Additionally, terrorist content appears on "dedicated websites, targeted virtual chat rooms and forums, online magazines, social networking platforms, such as Twitter, Facebook, and popular video and file-sharing websites, such as YouTube and Rapidshare, respectively." Terrorist propaganda focuses on the promotion of violence and/or extremist narratives, particularly in cyberspace. Online propaganda may include content that inspires young individuals to engage in role-play and develop an interest for terrorist activity. Consequently, this type of indoctrination poses a serious threat for internet users.

2. Psychological Operations

One of the major strategies used by terrorists is to evoke fear in members of the targeted population. The internet facilitates this process, since propaganda helps terrorist organizations share threatening messages through videos, online magazines and audio files. For example, Al-Qaeda and the Islamic State of Iraq and Syria (ISIS) regularly use media channels to disseminate messages and violent images that evoke fear. These include videos of beheadings, hostage takings, suicide bombings, explosions and calls for Jihad. Additionally, ISIS-affiliated 'Abd al Faqr media group published a guidebook and video providing religious justification for the use of biological weapons against "the enemy".

3. Incitement

Incitement to commit acts of terrorism or to assist in such acts takes place when terrorist groups or terrorists as individuals promote, encourage, urge or command such acts – whether or not they are eventually committed. As mentioned in the UNODC Report, there is a key distinction between propaganda and online material intended to incite individuals to commit acts of terrorism. For instance, in some jurisdictions, a direct causal relationship between propaganda and an actual terror plot (or attack) is necessary in order to be held liable for incitement to terrorism. Incitement that takes place via social media, websites, mobile phone communications, internet communications, and other cyber-enabled means shares similarities with incitement in the physical world.

One key aspect is the need to determine that such communications are not protected by free speech safeguards in the relevant jurisdiction. Examples of incitement to acts of terrorism in cyberspace include the dissemination of messages calling for a "holy war" against non-believers, when the messages are explicit and specific.

4. Recruitment

The internet facilitates the recruitment of terrorists and supporters of terrorism by enabling those who are most responsive to propaganda to develop radical views and join terrorist organizations. These organizations conduct both clandestine and open recruitment on websites, chat rooms and forums with restricted access to the general public. It is through these restricted platforms that potential recruits learn about the organization's purposes, ideologies, objectives and become more involved in terrorist activities. Recruiters know how to effectively indoctrinate marginalized and vulnerable individuals, including children. When targeting minors, propaganda may take the form of cartoons, music videos, and computer games that promote terrorist acts. Additionally, all the information used by terrorist organizations are available in many languages, enabling recruiters to reach a global pool of potential members.

5. Radicalization

Radicalization is the process by which recruits are transformed into individuals determined to act with violence on behalf of a terrorist organization. This is the stage in which recruits become involved and determined to adopt, conduct and live based on violent extremist ideologies. The radicalization process may be conducted online (in websites or chat-rooms) or offline (during one-on-one meetings).

6. Financing

Terrorist organizations use the internet to raise funds for their hostile activities. By employing effective propaganda strategies, they identify potential donors and instruct them about ways to financially support the organization. The UNODC Report indicates that they collect resources through the following ways: "direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations." Direct solicitation refers to the utilization of e-mails, online groups and websites by terrorists to demand donations from members. Additionally, websites are used as online stores, facilitating money transfers between parties. Terrorist organizations also exploit online payment facilities by stealing credit card information

or using other fraudulent means. Finally, charities or seemingly philanthropic organizations are misused by terrorists who collect donations for their own purposes.

7. Information Sharing

Terrorists use different online platforms to share information and provide potential recruits with training on how to conduct attacks. In many cases, they choose small or restricted-access platforms to ensure that their activities are not blocked by governments or private companies. Terrorists share audio files, electronic magazines, and videos to provide members with practical information on how to make explosives, or use firearms to stage attacks. For example, the Islamic State of Iraq and Syria (ISIS) had published on its online magazine "Rumiyah" instructions on how to perpetrate car ramming and stabbing attacks.

8. Intelligence

Studies have largely focused on terrorist use of the internet for radicalization and recruitment purposes, giving little attention to data mining and intelligence gathering. Yet terrorist organizations often use social media platforms to collect open-source intelligence on potential targets. This is key for them to effectively plan and coordinate their attacks. For instance, large-scale terrorist attacks such as the November 2015 Paris attacks carried out by the Islamic State of Iraq and Syria (ISIS) rely upon prior intelligence gathering and analysis by terrorist groups.

9. Communications

Terrorists use the internet to coordinate their daily activities and plan their operations. For example, Al-Qaeda used the internet in a number of ways to plan the September 11 attack against the United States that provoked that country's "war on terror". The internet also facilitates both ongoing communication between members of a terrorist organization and can be used specifically to support the planning stage of an attack. It also provides channels of communication that recommend ways to perpetuate attacks, and make instructional videos or audio files available. As seen in the cases of ISIS and Al-Qaeda, terrorist organizations use the internet to provide their members with tactics to effectively organize the preparatory steps of an attack.

10. Cyberterrorism

In circumstances where terrorist organizations may utilize the internet to inflict physical damage to property, including critical infrastructure such as electrical grids, water systems and railroads – such events may be classified as cyberterrorism, in accordance with many jurisdictions' definitions of terrorist acts. Certain countries have already used such cyber-enabled means to inflict physical damage, such as the Russian takedown of parts of the Ukrainian electrical grid in 2015 and 2016), or to cause loss of life or injury to people Some experts include the manipulation or destruction of non-physical data in this definition, as in the Syrian Electronic Army hack into an Associated Press Twitter account in April 2013 that caused a severe, albeit brief, drop in the value of stocks on the New York Stock Exchange. Such terrorist-initiated cyber attacks have been rare until now, for reasons that may include the small number of terrorist organizations that are capable of conducting such cyberattacks; and the lack of motivation on the part of terrorist organizations to focus on such operations due to reduced visibility of impact, as compared to operations carried out in the physical world.

Annex 2: Existing Laws Regarding Terrorist Use of the Internet

1. Propaganda

France – ***Code Pénal 421-2-5*** (Only French version available) "Le fait de provoquer directement à des actes de terrorisme ou de **faire publiquement l'apologie de ces actes** est puni de cinq ans d'emprisonnement et de 75 000 € d'amende"" & 421-2-5-1 ""**Le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme**"" & 421-2-6 ""I. c) Consulter habituellement un ou plusieurs services de communication au public en ligne ou **détenir des documents provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie".**

Germany – ***German Criminal Code***: Section 86: Dissemination of **propaganda** material of unconstitutional organizations & Section 131: Dissemination of **depictions** of violence & Section 166: Defamation of religions, religious and ideological associations - **Additionally, the Network Enforcement Act states in Section 1/1 that: "telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public" are responsible for deleting "Unlawful content" (1/3) related to terrorism or other extremist causes**. ++Section 2 (paragraphs 2) of the *Counter-Terrorism File Law* defines terrorists as "individuals that unlawfully use, prepare or support violence as a means of enforcing internationally oriented political or religious concerns, or intentionally causing them by their activities, in particular by advocating such use of force".

Israel – According to Article 24 of the ***Counter-Terrorism Law, 5776-2016*** (24. Demonstrating identification with a terrorist organization and incitement to terrorism): "Article 24 (a): “One who commits an act of identification with a terrorist organization, including by **publishing words of praise, support or sympathy**, waving a flag, **displaying or publishing a symbo**l, or displaying, playing or **publishing a slogan or anthem**, in one of the following [situations], is liable to three years' imprisonment”.

Article 24 (b): “One who **publishes a direct call to commit a terrorist act**” (1) or “one who **publishes praise, sympathy, encouragement or support of a terrorist actor identification with it**, where the content of the publication and the circumstances in which it was published, give rise to a substantial possibility that it will bring about the commission of a terrorist act” (2) “is liable to five years’ imprisonment”. +++ ***Prevention of Terrorism Ordinance No. 33 of 5708- (1948), §2:*** "delivering a **propaganda** speech a public meeting or over the **wireless** on behalf of a terrorist organization shall be guilty of an offence".

United Kingdom – ***Terrorism Act 2006 as amended by the new Counter Terrorism and Border Security Act 2019*** **- Encouragement of terrorism, Section 1** - "This section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as **a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism** or Convention offences (2) A person commits an offence **if (a) he publishes a statement** to which this section applies or causes another to publish such a statement;(b) at the time he publishes it or causes it to be published, he— (i) **intends members of the public to be directly or indirectly encouraged** or otherwise induced by the statement to commit, prepare or instigate acts of terrorism or Convention offences; or (ii) is reckless as to whether **members of the public will be directly or indirectly encouraged** or otherwise induced by the statement to commit, prepare or instigate such acts or offences." Section 3 - For the purposes of this section, the statements that are likely to be understood by members of the public as indirectly encouraging the commission or preparation of acts of terrorism or Convention offences include every statement which—(**a)glorifies the commission or preparation** (whether in the past, in the future or generally) of such acts or offences; and (b)is a statement from which those members of the public could reasonably be expected to infer that what is **being glorified** is being glorified as conduct that should be emulated by them in existing circumstances. **Terrorism Act 2006 as amended by the new Counter Terrorism and Border Security Act 2019 - Dissemination of terrorist publications** - Section 2 - (1) A person commits an offence if he engages in conduct falling within subsection (2) and, at the time he does so— (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;** (b) he intends an effect of his conduct

to be **the provision of assistance in the commission or preparation of such acts**; or (c) he is reckless as to whether his conduct has an effect mentioned in paragraph (a) or (b). (2) - For the purposes of this section a person engages in conduct falling within this subsection if he—(a) distributes or circulates a terrorist publication; (b) gives, sells or lends such a publication; (c) offers such a publication for sale or loan; (d) provides a service to others that enables them to obtain, read, listen to or look at such a publication, or to acquire it by means of a gift, sale or loan; (e) transmits the contents of such a publication electronically; or (f) has such a publication in his possession with a view to its becoming the subject of conduct falling within any of paragraphs (a) to (e). **Counter Terrorism and Border Security Act 2019** adds to the Terrorism Act 2006 following statements: In section 2, subsection (3), in paragraph (a) "For the purposes of this section **a publication is a terrorist publication**, in relation to conduct falling within subsection (2), if matter contained in it is likely— (a) to be understood, by some or all of the persons to whom it is or may become available as a consequence of that conduct, as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism; for the words from ", by" to "them" substitute "by a reasonable person as a direct or indirect encouragement or other inducement, to some or all of the persons to whom it is or may become available as a result of that conduct,".

United States – ***First Amendment*** - Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." **+** ***Cases in which it is not applicable***: In ***Brandenburg v. Ohio 1969***, US courts determined that free speech is not protected when it is **"directed to inciting or producing imminent, lawless action and likely to incite or produce such imminent action"**. + The federal courts had to address a claim by the Humanitarian Law Project that the material support statute (18 U.S.C. §2339B) violated the First Amendment by punishing speech acts (i.e., its provision of training on international humanitarian law to two organizations the U.S. government had designated as foreign terrorist organizations (the PKK and LTTE). The case went to the Supreme Court, which, **in Holder vs. Humanitarian Law Project (130 S.Ct. 2705 (2010))** held by a 6-3 majority that the material support statute did not, in this case, violate the First Amendment. Writing for the majority, Chief Justice Roberts

framed the First Amendment issue as a question of whether the government could prohibit material support to the PKK and LTTE in the form of speech acts (e.g., training). The majority held that deference to Congress and the Executive Branch was necessary concerning whether training in non-violent, legal skills aided terrorist activities. + ***Miller v. California, 413 U.S. 15 (1973)*** **- Obscenity**: "Every person who knowingly: sends or causes to be sent, or brings or causes to be brought, into this state for **sale or distribution, or in this state prepares, publishes, prints, exhibits, distributes, or offers to distribute, or has in his possession with intent to distribute or to exhibit or offer to distribute, any obscene matter is guilty** of a misdemeanor." + ***Near v. State of Minnesota Ex Rel. Olson, 283 U.S. 697 (1931) - Defamation:*** Any person who, as an individual, or as a member or employee of a firm, or association or organization, or as an officer, director, member or employee of a corporation, shall be engaged in the business of regularly or customarily **producing, publishing or circulating, having in possession, selling or giving away**. (a) **an obscene, lewd and lascivious newspaper, magazine, or other periodical, or (b) a malicious, scandalous and defamatory newspaper, magazine or other periodical, is guilty of a nuisance, and all persons guilty of such nuisance may be enjoined, as hereinafter provided. + *Dennis v. United States, 341 U.S. 494 (1951)*** **- Sedition:** "where one of the "acts" which the Court found the **government could prohibit** was to knowingly and willfully "a**dvocate and teach the duty and necessity of overthrowing and destroying the Government** of the United States by **force and violence."**

European Union ***–Art. 5 Directive (EU) 2017/541 "Public provocation to commit a terrorist offence***" demands Members States to take "necessary measures to ensure that the **distribution**, or otherwise **making available by any means**, whether **online or offline**, of a **message to the publi**c, with the **intent to incite the commission** of one of the offences listed in points (a) to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the **glorification of terrorist acts**, **advocates** the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally." ***Article 2(5) of the Proposal for a Regulation on preventing the dissemination of terrorist content online*** defines ‘terrorist content’ as: "(a) i**nciting or advocating**, including by **glorifying**, the commission of terrorist offences, thereby causing a danger that such acts be committed".

United Nations – ***UN Resolution 2178 (2014)*** recognizes that terrorists' increasing use of information and communications technology for **recruitment and propaganda poses significant challenges for policymakers and law enforcement agencies around the world. ++++ *Security Council resolutions 1373 (2001) and 1624 (2005)* emphasize the need to strengthen international cooperation in countering the use of the Internet and social media for terrorist purposes.** However, efforts to achieve a global legal consensus continue to be undermined by significant differences between Member States' relevant domestic legislation and the limited capacity of investigators and prosecutors to access electronic evidence.

NATO – none.

OSCE - none.

2. Psychological Operations

France - ***French Penal Code***: Article 421-1 (Under the definition of Terrorist Act) "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 public order through intimidation or terror**: .....

Germany - ***German Criminal Code:*** Section 129a: "any person who participates in such a group as a member, if one of the offences stipulated in Nos 1 to 5 is intended to **seriously intimidate the population,** to unlawfully coerce a public authority or an international organisation through the use of force or **the threat** of the use of force" + ***German Criminal Code***: Section 131 "disseminates written materials, which describe cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner **expressing glorification**" + ***The Network Enforcement Act "NetzDG"***: Article 1 "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel - According to Article 2 of the ***Counter-Terrorism Law, 5776-2016*** (2. Definitions and Interpretation): "a Terrorist Act" is an act that constitutes an offense, or a threat to carry out such an act, which meets all of the following: "(1) It was carried out with a political, religious, nationalistic or ideological motive; (2) It was **carried out with the intention of provoking fear or panic among the public** or with the **intention of compelling a government** or other governmental authority, including a government or other governmental authority of a foreign country, or a public international organization, to do or to abstain from doing any act; (3) The act carried out **or threatened to be carried out**, involved one of the following, or posed an actual risk of one of the following: a) Serious harm to a person's body or freedom ; b) Serious harm to public health or safety...". +++ ***Prevention of Terrorism Ordinance No. 33 of 5708-(1948), §1:*** ""Terrorist organisation" means a body of persons resorting in its activities to acts of violence calculated to cause death or injury to a person or to **threats of such acts of violence**".

United Kingdom - **none.**

United States - The United States **f*ederal law***'s definition of "international terrorism" includes activities that "...**intimidate or coerce a civilian population...**"; "...influence the policy of a government by **intimidation or coercion...**"; or "...affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or **transcend national boundaries in terms of the means by which they are accomplished**, the persons they appear **intended to intimidate or coerce**, or the locale in which their perpetrators operate or seek asylum". The United States definition of "domestic terrorism" includes activities that "....**intimidate or coerce** a civilian population...";"...influence the policy of a government by intimidation or coercion...". The US definition of a "federal crime of terrorism" is one that: "...is calculated to influence or affect the conduct of government by **intimidation or coercion**, or to retaliate against government conduct...". +++ First established in ***Watts v. United States (1969)***, "true threat" is a key doctrine that can apply to many terrorist activities on the web. The doctrine dictates that speech is not protected when a person "knowingly and willfully . . . **[making] any threat to take the life of or to inflict bodily harm** upon the President of the United States (...)". + ***Schenck v. United States, 249 U.S. 47 (1919)*** **-Causing panic:** "The

most stringent protection of free speech would not protect a man in **falsely shouting fire in a theatre and causing a panic.**"

European Union - ***Art. 3 Directive (EU) 2017/541 "Terrorist offences"*** states that Member States have the responsibility to "take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2: (a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person; ... (j) **threatening to commit** any of the acts listed in points (a) to (i). 2. The aims referred to in paragraph 1 are: (a) **seriously intimidating** a population; (b) unduly **compelling** a government or an international organisation **to perform or abstain from** performing any act; +(10) The offence of public provocation to commit a terrorist offence act comprises, inter alia, the glorification and justification of terrorism or the dissemination of messages or images **online and offline**, **including those related** to the victims of terrorism as a way to gather support for terrorist causes or **to seriously intimidate the population**.

United Nations - none.

NATO - none.

OSCE - OSCE has adopted the definition provided by the United Nations and recognized in the **UN Security Council Resolution 1566 (2004**) which describes acts of terrorism as: " ...criminal acts, including against civilians, **committed with the intent to** ... **intimidate** a population **or compel** a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature".

3. Incitement

France - ***Code Pénal*** (only available in French): Article 421-2-4: **Le fait d'adresser à une personne** des offres ou des promesses, de lui proposer des dons, présents ou avantages quelconques, **de la menacer ou d'exercer sur elle des pressions afin qu'elle participe à un groupement ou une entente prévu à l'article 421-2-1 ou qu'elle commette un des actes de terrorisme** mentionnés aux articles 421-1 et 421-2 est puni, même lorsqu'il n'a pas été suivi d'effet, de dix ans d'emprisonnement et de 150 000 € d'amende.

Germany - ***German Criminal Code***: Section 91: **Encouraging** the commission of a serious violent offence endangering the state & Section 111: Public **incitement to crime** & Section 130: **Incitement to hatred** & Section 130a: "(1) Whosoever disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3))... intended by its content **to encourage or cause others to commit such an act**..." & Section 357: **Incitement** of a subordinate to the commission of offences. + Section 2 (paragraphs 2) of the Counter-Terrorism File Law defines terrorists as "individuals that unlawfully use, prepare or support violence as a means of enforcing internationally oriented political or religious concerns, or intentionally causing them by their activities, in particular by **advocating such use of force**". + ***The Network Enforcement Act "NetzDG"***: Article 1 "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel - ***Israel Penal Law***, 5737-1977: Chapter Eight: Offenses Against the Political and Social Order - Incitement to violence or terror 144D2.(a) "If a person **publishes a call to commit an act of violence**, or praise, words of approval, encouragement, support or identification with an act of violence (in this section: inciting publication) and if – because of the inciting publication's contents and the circumstances under which it was made public **there is a real possibility that it will result in acts of violence**, then he is liable to five years imprisonment." +++ Additionally, ***Article 24 of the Counter-Terrorism Law, 5776-2016*** (24. Demonstrating identification with a

terrorist organization and **incitement to terrorism**) makes it illegal to incite to terrorism: Article 24 (a): "One who commits an act of identification with a terrorist organization, including by publishing words of praise, support or sympathy, waving a flag, displaying or publishing a symbol, or displaying, playing or publishing a slogan or anthem, in one of the following [situations], is liable to three years' imprisonment". Article 24 (b): "One who **publishes a direct call to commit a terrorist act**" (1) or "one who publishes praise, sympathy, encouragement or support of a terrorist act, or identification with it, **where the content of the publication and the circumstances in which it was published, give rise to a substantial possibility that it will bring about the commission of a terrorist act**" (2) "is liable to five years' imprisonment".

United Kingdom - ***Terrorism Act 2006 as amended by the new Counter Terrorism and Border Security Act 2019 - Encouragement of terrorism, Section 1*** - "This section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a **direct or indirect encouragement or other inducement to them to the commission**, preparation or instigation of acts of terrorism or Convention offences (2) A person commits an offence if (a) he publishes a statement to which this section applies or causes another to publish such a statement;(b) at the time he publishes it or causes it to be published, he— **(i) intends members of the public to be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate acts of terrorism** or Convention offences; or (ii) is reckless as to whether members of the **public will be directly or indirectly encouraged or otherwise induced** by the statement to commit, prepare or instigate such acts or offences." Section 3 - For the purposes of this section, the statements that are likely to be understood by members of the public as **indirectly encouraging the commission or preparation of acts** of terrorism or Convention offences include every statement which—(a)glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences; and (b)is a statement from which those members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances. ***Terrorism Act 2006 as amended by the new Counter Terrorism and Border Security Act 2019 - Dissemination of terrorist publications*** - Section 2 - (1) A person commits an offence if he engages in conduct falling within subsection (2) and, at the time he does so— (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;

United States - In ***Brandenburg v. Ohio 1969***, US courts determined that free speech is not protected when it is "directed to inciting or producing imminent, lawless action and l**ikely to incite** or produce such imminent action". +++ Terrorism as defined in ***The Patriot Act (2001)*** §411 (B) (ii) P346- "to commit or to **incite to commit**, under circumstances indicating an intention to cause death or serious bodily injury, **a terrorist activity**..."+ **D*ennis v. United States, 341 U.S. 494 (1951)* - Sedition:** "where one of the "acts" which the Court found the government could prohibit was to knowingly and willfully "a**dvocate and teach the duty and necessity of overthrowing and destroying the Government of the United States by force and violence." +** ***Chaplinsky v. New Hampshire, 315 U.S. 568 (1942)*** **- "Fighting words**: The U.S. Supreme Court held that the First Amendment **does not protect "fighting words -- those which by their very utterance inflict injury or tend to incite an immediate breach of the peace."**

European Union - ***Directive (EU) 2017/541*** - Article 5 **Public provocation to commit a terrorist offence:** "Member States shall take the necessary measures to ensure that the distribution, or otherwise making available by any means, whether **online or offline**, of a message to the public, **with the intent to incite the commission of one of the offences listed in points** (a) to (i) of Article 3(1), where such conduct, **directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences**, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally." Article 14 **Aiding and abetting, inciting and attempting:** 2. Member States shall take the necessary measures to ensure that **inciting an offence** referred to in Articles 3 to 12 is punishable. (Article 3 - **Terrorist offences**, Article 12 - **Other offences related to terrorist activities**)"+++***EU Parliament Resolution on Prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015)*** - "15. calls for an **effective strategy for the detection and removal of illegal content inciting to violent extremism**, while respecting fundamental rights and freedom of expression, and in particular for contributing to the dissemination of effective discourse to counter terrorist propaganda."

United Nations - ***Security Council resolution 2178 (2014)*** - **C. Countering incitement to terrorism, including through the Internet** :60. Nearly all the States surveyed have taken steps to **prohibit incitement to terrorism under their criminal laws**, as called for by resolution 1624 (2005). Those measures can contribute significantly to stemming the flow of foreign terrorist fighters, since foreign terrorist fighters are **often spurred to action by calls to terrorist violence made by others, either in person or through the Internet or other social media**. **Certain restrictions on the 34 right to freedom of expression, subject to strict requirements, may legitimately be applied, including in cases of terrorist incitement.** +++ ***The United Nations Office on Drugs and Crime*** - **The use of the internet for terrorist purposes:** "10**.** While propaganda per se is not generally prohibited, **the use of propaganda by terrorists to incite acts of terrorism is considered unlawful by many Member States**. The Internet provides an abundance of material and opportunities to download, edit and distribute content that may be considered **unlawful glorification of, or provocation to, acts of terrorism.** 34. As noted in subsection B.1(b) above, the **proscription of incitement to terrorism may involve restrictions on freedom of expression. Freedom of expression is not an absolute right.** It may be restricted, subject to satisfaction of strictly construed tests of legality, necessity, proportionality and non-discrimination, when that freedom is used to incite discrimination, hostility or violence. "

NATO - none.

OSCE - ***Resolution on Preventing and Countering Terrorism and Violent Extremism and Radicalization that lead to terrorism.*** p.2: "Deploring all the acts, methods and practices of terrorism... and also **condemning the incitement of terrorist acts**, and repudiating attempts at the justification or glorification of terrorist acts that may incite further terrorist acts". ***The Ministerial Council Declaration No. 5/14 on The OSCE Role in Countering the Phenomenon of Foreign Terrorist Fighters in the Context of the Implementation of UN Security Council Resolutions 2170 (2014) and 2178 (2014) (MC.DOC/5/14)*** mentions the goal to promote public-private partnerships with civil society, the media, the business community, and industry in countering terrorism, in line with, inter alia, Ministerial Council Decision No. 10/08, i**n order to counter the incitement,** recruitment, and travel of foreign terrorist fighters, as well as to prepare for

and mitigate the threat posed by their return. Additionally, In **Ministerial Council Declaration No. 1,** OSCE declares that there i**s a need to address the threat posed by narratives used by terrorists, including public justification of terrorism, incitement and recruitment**, and call on the participating States to act co-operatively to develop the most effective responses to this threat, in compliance with international law, including international human rights law."

4. Recruitment

France - ***French Penal code***: Chapter VI - Taking part in mercenary activity Art. 436-1 (Inserted by Act no. 2003-340 of 14 April 2003. Art. 1 Official Journal of 15 April 2003): The following are punished by five years' imprisonment and by a fine of €75,000: "1º For any **person who has been specially recruited to participate in an armed conflict**, and who is neither a citizen of a State involved in the aforesaid conflict, nor a member of the armed forces of the State, and has not been sent on a mission by another State not involved in the conflict as a member of the armed forces of this State, to directly participate or to attempt to directly participate in the hostilities, with a view to obtaining personal advantage or remuneration considerably in excess of what is paid or promised to the combatants of the same rank and with the same duties in the armed forces fighting on the same side; 2º For any **person who has been specially recruited to take part in a concerted violent act designed to overthrow institutions or to attack the territorial integrity of a State**, and who is not a citizen of the State against which the attack is planned, nor a member of the aforesaid State's armed forces, and who has not been sent on such a mission by another State, to take part in such an act with a view to obtaining a personal advantage or a significant payment."

Germany - ***German Criminal Code***: Section 129a: Forming terrorist organisations: "Whosoever **recruits members** or supporters for a group as described in subsection (1) or subsection (2) above shall be liable to imprisonment from six months to five years." & Section 109f: Intelligence activity endangering national security: "(1) Whosoever, on behalf of a government agency, a party or another organisation outside the Federal Republic of Germany or for a banned organisation or one of its intermediaries" (3) **recruits for** or supports one of these activities & Section 109h: Recruiting for foreign

armed forces: (1) "Whosoever on behalf of a foreign power **recruits a German for military service in a military or paramilitary organisation** or introduces him to their recruiters or to the military service of such an organisation...". + ***The Network Enforcement Act "NetzDG"***: Article 1 "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel- Article 22 of the ***Counter-Terrorism Law, 5776-2016*** (22. Membership in a Terrorist Organization and Recruitment of Members): "(a)One who is a **member of a terrorist organization** is liable to five years' imprisonment. (b)A member of a terrorist organization who takes part in the organization's activity, or who performs an activity on behalf of the organization or with the intention of promoting its activity, is liable to seven years' imprisonment. (c)**One who recruits a member to a terrorist organization, directly or indirectly**, is liable to seven years' imprisonment."

United Kingdom - ***Terrorism Act 2000 as amended by the Counter Terrorism and Border Security Act 2019*** - c.11, Part II, Offences Section 12 - **Support - "**(1A) A person commits an offence if the person— (a) expresses an **opinion or belief that is supportive of a proscribed organisation**, and (b) in doing so is reckless as to whether **a person to whom the expression is directed will be encouraged to support a proscribed organisation**." (2)A person commits an offence if he **arranges, manages or assists in arranging or managing a meeting** which he knows is— (a)to support a proscribed organisation, (b)to further the activities of a proscribed organisation, or **(c)to be addressed by a person who belongs or professes to belong to a proscribed organisation** (3) **A person commits an offence if he addresses a meeting and the purpose of his address is to encourage support for a proscribed organisation or to further its activities.**

United States - none.

European Union - ***Art. 6 Directive (EU) 2017/541 "Recruitment for terrorism*** - Member States shall take the necessary measures to ensure that **soliciting another person to commit or contribute to the commission** of one of the offences listed in

points (a) to (i) of Article 3(1), or in Article 4 is punishable as a criminal offence when committed intentionally.**" + *European Parliament resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI))* - "13.** Encourages the establishment of educational programmes with adequate funding in European prisons in order to promote critical thinking, religious tolerance, and reintegration into society of inmates, **but also to offer special assistance to those who are young, vulnerable or more susceptible to radicalisation and recruitment by terrorist organisations**, and thus on a basis of the utmost respect for the human rights of inmates; considers that accompanying measures should also be offered subsequently to release from prison...". + ***Art. 31 Directive (EU) 2017/541 "Recruitment for terrorism*** "As reflected in the revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism of 2014 and in the Conclusions of the Council of the European Union and of the Member States meeting within the Council on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism of 2015, prevention of radicalisation and recruitment to terrorism, including radicalisation online"

United Nations - ***Security Council resolution 2178 (2014)*** lays out specific procedures to **combat offline and online recruitment alike, with the main focus on the terrorist foreign fighters**. In Chapter II/A it rules that "the technological advances of the past decade have created an environment in which individuals are able to freely interact with counterparts worldwide, including with malevolent actors, and instantaneously project their views and ideologies, at little or no cost." Especially "the Islamic State in Iraq and the Levant (ISIL) has taken full advantage of the Internet and social media to disseminate its ideology, publicize its activities, raise funds and coordinate and develop its operations." ***While the resolutions 1373 (2001), 1624 (2005) and 2178 (2014)*** reflect the global consensus on the urgent need to strengthen international cooperation in countering the use of the Internet and social media for terrorist purposes, **in particular foreign terrorist fighter recruitment**, there is no clear consensus as to what measures may and should be taken.

NATO - none.

OSCE - ***Ministerial Council Declaration No. 1*** on Strengthening OSCE Efforts to Prevent and Counter Terrorism (MC.DOC/1/16): "We stress that **participating States** have the **primary role in preventing and countering terrorism and violent extremism and radicalization that lead to terrorism (VERLT)**, while respecting their obligations under international law, in particular human rights and fundamental freedoms. (…) We recognize that participating States should take measures, consistent with their OSCE commitments, and while ensuring national ownership, to address the conditions conducive to the spread of terrorism, while recognizing that none of these conditions can excuse or justify acts of terrorism. In this context, we recognize the **need to address the threat posed by narratives used by terrorists**, including **public justification of terrorism, incitement and recruitment, and call on the participating** States to act co-operatively to develop the most effective responses to this threat, in compliance with international law, including international human rights law." +++ ***DECISION No. 1063 OSCE CONSOLIDATED FRAMEWORK FOR THE FIGHT AGAINST TERRORISM (2012)***, p.4: " the OSCE will pursue activities designed to help eliminate the conditions in which terrorists may win support and engage in recruitment, including through: – Addressing negative socio-economic factors..." +++ ***PC Journal No. 934, Agenda item 1, (2012),*** p.5: "Counter violent extremism and all forms of radicalization leading to terrorism, as well as **stem recruitment** and training for terrorism;" ***The Ministerial Council Declaration No. 5/14 on The OSCE Role in Countering the Phenomenon of Foreign Terrorist Fighters in the Context of the Implementation of UN Security Council Resolutions 2170 (2014) and 2178 (2014) (MC.DOC/5/14)*** mentions the goal to promote public-private partnerships with civil society, the media, the business community, and industry in countering terrorism, in line with, inter alia, ***Ministerial Council Decision No. 10/0***8, in order to counter the incitement, r**ecruitment, and travel of foreign terrorist fighters, as well as to prepare for and mitigate the threat posed by their return.** Additionally, In **Ministerial Council Declaration No. 1**, OSCE declares that there is a need to address the threat posed by narratives used by terrorists, including public justification of terrorism, incitement a**nd recruitment, and call on the participating States to act co-operatively to develop the most effective responses to this threat**, in compliance with international law, including international human rights law."

5. Radicalization

France - none.

Germany - none.

Israel - none.

United Kingdom - none.

United States - none.

European Union - *European Parliament resolution of 25 November 2015* on the **prevention of radicalisation and recruitment of European citizens by terrorist organisations** (2015/2063(INI)) + **III. Preventing online terrorist radicalisation. +** ***Art. 31 Directive (EU) 2017/541 "Recruitment for terrorism*** "As reflected in the revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism of 2014 and in the Conclusions of the Council of the European Union and of the Member States meeting within the Council on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism of 2015, prevention of radicalisation and recruitment to terrorism, including radicalisation online"

United Nations - *Security Council resolution 2178 (2014)* 26. Some States continue to develop **counter-messaging approaches in order to challenge and refute messages supporting or glorifying terrorist activity.** Others are proactively producing alternative messages (e.g. retelling and amplifying positive narratives that advocate peace, respect and social inclusion, or deconstructing the narratives of terrorists). E**ffective strategies to counter the threat of online radicalization to terrorism require that Governments act beyond legislative and law enforcement measures to engage with communities and industry.** In most cases, the most effective conveyors of counter-narratives may be family and friends, civil society actors, academic institutions, religious or community leaders and other non-governmental actors. For such campaigns to be effective, **the private sector (because of its intimate knowledge of social media demographics and marketing tools) should be an active participant.** Governments should welcome grass-roots campaigning initiatives and support them.

NATO - none.

OSCE - ***Ministerial Council Declaration No. 4/15*** on **Preventing and Countering Violent Extremism and Radicalization** that Lead to Terrorism (MC.DOC/4/15) (…) Underscoring the commitment of **participating States to take the measures needed to protect everyone within their jurisdiction against terrorist acts**, and to take resolute action to counter terrorism and foreign terrorist fighters, including by fully implementing UNSCR 2170, 2178, 2199 and 2249, with regard to the terrorist groups identified therein, in support of our relevant OSCE commitments, and in compliance with applicable obligations under international law, including international human rights law, international refugee law and international humanitarian law, (…) +++ ***DECISION No. 1063 OSCE CONSOLIDATED FRAMEWORK FOR THE FIGHT AGAINST TERRORISM (2012)***, p.5: "Counter violent extremism and **all forms of radicalization** leading to terrorism, as well as stem recruitment and training for terrorism;"

6. Financing

France - ***French Penal Code***: Art. 421-2-2 CP condemns as an act of terrorism the financing of a terrorist group "by **providing, collecting or managing funds**, securities or property of any kind, or by giving advice for this purpose, intending that such funds, security or property be used, or knowing that they are intended to be used, in whole or in part, for the commission of any of the acts of terrorism listed in the present chapter, irrespective of whether such an act takes place." (keeping in mind that the definition of a terrorist act includes computer offenses) Art. 421-1 CP French Penal Code: The definition of terrorist act includes 4° "...the production, **sale,** import or export of explosive substances [...]; - **the purchase**, keeping, transport or unlawful carrying of explosive substances or of devices made with such explosive substances..." - "...the offences defined by articles 1 and 4 of the Act no. 72-467 of 9 June 1972 forbidding the designing, production, keeping, stocking, **purchase or sale of biological or toxin-based weapons...".** 6° the **money laundering offences** set out in Chapter IV of title II of Book III of the present Code. 7° the insider **trading offences** set out in article L.465-1 of the Financial and Monetary Code."

Germany - ***German Criminal Code:*** Section 261 **Money laundering**; hiding unlawfully obtained financial benefits - "misdemeanours under section 89a and under section 129 and section 129a (3) and (5), all of which also in conjunction with section 129b (1), as well as misdemeanours **committed by a member of a criminal or terrorist organisation** (section 129 and section 129a, all of which also in conjunction with section 129b (1))" + ***The Network Enforcement Act "NetzDG"***: Article 1 "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel - According to the ***Counter-Terrorism Law, 5776-2016***: (2. Definitions and Interpretation), a "terrorist organization" is "...(2) A body of persons in an organized and continuous structure that acts, directly or indirectly**, to assist an organization mentioned in paragraph (1),** or that acts with **the intention of promoting the activity of such an organization**, including by **financing it** – **all of the foregoing**, in a manner capable of making a substantial or ongoing **contribution to the organization's activity**, or [where such body of persons] has a substantial affiliation to [the organization], provided that the body of persons [defined in this paragraph] has been designated as a terrorist organization pursuant to Part B..." +++ ***Prevention of Terrorism Ordinance No. 33 of 5708- (1948), §1***: ""member of a terrorist organisation" means a person ... c**ollecting moneys or articles** for the benefit of a terrorist organisation or activities." "terrorist financing" (**Crime - Overseas Production Orders Act 2019!)**

United Kingdom - ***Terrorism Act 2000*** c.11, Part III, offences, Section 15 - Fund-raising - (1) A person commits an offence if he (a) invites another to **provide money or other property**, and (b) intends that it should be used, or has reasonable cause to suspect that it may be **used, for the purposes of terrorism**. (2)A person commits an offence if he— (a) receives money or other property, and (b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism. +++ Section 18 - Money laundering. (1)A person commits an offence if he enters into or becomes concerned in an arrangement which **facilitates the retention or control by or on behalf of another person of terrorist property— (a)by**

concealment, (b)by removal from the jurisdiction, (c)by transfer to nominees, or (d)in any other way. +Sections from **24 to 31** all additionally **deal with the seizing of terrorist cash.+** ***Crime (Overseas Production Orders) Act 2019*****:** Making of **overseas production order on application** (1) A judge may, on an application by **an appropriate officer, make an overseas production order against a person in respect of electronic data** if each of the requirements for the making of the order is fulfilled - (4) A Schedule 5A **counter-terrorism financial investigator may exercise** a function conferred by a provision of this Act only if exercising the function for the **purposes of a terrorist financing investigation.**

United States - According to the ***U.S. Code §2339A*** (relating to providing material support to terrorists): "Whoever provides **material support or resources** or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section ... or any offense listed in section ***2332b*****(g)(5)(B)** (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title...". "...(1) the term **"material support or resources" means** any property, tangible or intangible, or service, **including currency or monetary instruments or financial securities, financial services,** lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials...". +++ ***U.S Code §2339B*** (Providing material support or resources to designated foreign terrorist organizations): "...Whoever knowingly provides material support or resources to a foreign terrorist organization...". 2339C (relating to **financing of terrorism**), 2339D (relating to military-type training from a foreign terrorist organization)..." ++++ Amendments to ***2339C*** **of the US Code - SEC. 6604. FINANCING OF TERRORISM.** (a) FINANCING TERRORISM.— Section 2339c(c)(2) of title 18, United States Code, is amended— (1) by striking ‘‘, resources, or funds’’ and inserting ‘‘or resources, or **any funds or proceeds of such funds**’’; (2) in subparagraph (A), by striking ‘‘were provided’’ and inserting ‘‘**are to be provided, or knowing that the support or resources were provided**,’’; and (3) in subparagraph (B)— (A) by striking ‘‘or any proceeds of such funds’’; and (B) by

striking ‘‘were provided or collected’’ and inserting ‘‘**are to be provided or collected, or knowing that the funds were provided or collected**,’’.

<u>European Union</u> - ***Art. 6 (EU) Directive 2017/541 :*** "The definition of terrorist offences, of offences related to a terrorist group and of offences related to terrorist activities should be further approximated in all Member States, so that it covers conduct related to, in particular, foreign terrorist fighters and terrorist financing more comprehensively. **These forms of conduct should also be punishable if committed through the internet**, including social media." +***Art. 11 (EU) Directive 2017/541 "Terrorist financing*** - Member States shall take the necessary measures to ensure that **providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of**, any of the offences referred to in Articles 3 to 10 is punishable as a criminal offence when committed intentionally." + ***European Parliament resolution of 25 November 2015*** *on* ***the prevention of radicalisation and recruitment of European citizens by terrorist organisations*** (2015/2063(INI)) - 64. Calls on the EU to i**ncrease its cooperation with regional partners in order to curb arms trafficking, targeting in particular the countries where terrorism originates**, and to **follow closely the export of armaments that could be exploited by terrorists**; also calls for foreign policy tools and engagement with third countries to be strengthened with a view to **countering the financing of terrorist organisations**; draws attention to the conclusion of the G20 Summit of 16 November 2015, which calls on the Financial Action Task Force (FATF) to act more swiftly and efficiently when it comes to cutting off funding for terrorist organisations.

<u>United Nations</u> - ***The International Convention for the Suppression of the Financing of Terrorism of 1999*** ruled that all States should **"take steps to prevent and counteract (...) the financing of terrorists and terrorist organizations, whether such financing is direct or indirect** through organizations (...) including the **exploitation of persons for purposes of funding terrorist activities (...).** Commits States to hold those who finance terrorism criminally, civilly or administratively liable for such acts; and **provides for the identification, freezing and seizure of funds allocated for terrorist activities**, as well as for the sharing of the forfeited funds with other States on a case-by-case basis." **+++** ***Security Council resolution 2178 (2014)*** **-**

"Gaps remain in Member States' **legislation on countering the financing of terrorism and measures to freeze terrorist assets.** There is an **increasing need for Member States' anti-money-laundering/combating the financing of terrorism regulators to engage with financial institutions to communicate potential red flags that may indicate financial activity that supports ISIL and groups associated with Al-Qaida in order to prevent those groups and groups associated with Al-Qaida from accessing the international financial system.**" +++ ***Security Council resolution 1373 (2001)*** : 1.(a) "All States shall prevent and suppress the **financing of terrorist act**".

NATO- ***Brussels Summit Declaration 2018*** : (point 10) "We condemn all financial support of terrorism"

OSCE- ***DECISION No. 1063 OSCE CONSOLIDATED FRAMEWORK FOR THE FIGHT AGAINST TERRORISM (2012)***, p.5: "Suppress the financing of terrorism, including its linkages with money-laundering and illegal economic activities..." +++ ***Resolution on Preventing and Countering Terrorism and Violent Extremism and Radicalization that lead to terrorism,*** p.2: "Underlining the need to prevent and **suppress terrorist financing** through enhanced international and regional co-operation within the UN, the OSCE, the Financial Action Task Force (FATF) and FATF-style regional bodies". 9. Reaffirming that those who **participate in the financing**, planning, facilitating, preparing or perpetrating terrorist acts **must be held accountable and brought to justice**, on the basis of the principle "extradite or prosecute" in compliance with relevant obligations under international law, as well as applicable domestic legislation. 18. Calling urgently for a strengthening of the **measures against the financing of international terrorist groups**, in accordance with the **International Convention for the Suppression of the Financing of Terrorism**, and urging the swift and effective i**mplementation of the Financial Action Task Force's (FATF) standards**.

7. Information Sharing

France - ***Code Pénal*** Art.421-2-6 I. 2° b) Constitue un acte de terrorisme...."**S'entraîner ou se former** au maniement des armes ou à toute forme de

combat, à la fabrication ou à l'utilisation de substances explosives, incendiaires, nucléaires, radiologiques, biologiques ou chimiques ou au pilotage d'aéronefs ou à la conduite de navires"

Germany - ***German Criminal Code:*** Section 130a: Attempting to cause the commission of offences by means of publication. "(1) Whosoever disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) **capable of serving as an instruction** for an unlawful act named in section 126(1) and intended by its content to encourage or cause others to commit such an act, shall be liable to imprisonment not exceeding three years or a fine." + ***German Criminal Code*** Section 89b (1) "Whosoever, with the intention of **receiving instruction for the purpose of the commission of a serious violent offence endangering the state** under section 89a(2)". + ***The Network Enforcement Act "NetzDG"***: Article 1 "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel - According to the ***Counter-Terrorism Law, 5776-2016***: (2. Definitions and Interpretation), "a Terrorist Organization" – is "...(1) A body of persons in an organized and continuous structure that commits terrorist acts or that operates with the intention that terrorist acts will be committed — including an aforementioned body of persons that is engaged in **training or instruction** for the commission of terrorist acts...". ++ Additionally, ***Article 25 of the Counter-Terrorism Law*** (25. Providing Resources for Committing a Terrorist Act): "...(2)Providing another with money, food, clothing, **information**, means of communication, documents, vehicles, gasoline, land, a structure, or any other resource...". ++ *Article 29 of the Counter-Terrorism Law* (29. Training or instruction for the purposes of terrorism): "(a)**One who trains or instructs another to use operational methods or means to commit an offense that is a terrorist act ... or who trains or instructs another to use or prepare weapons**, and all of the above, with the intention of advancing or assisting the activity of a terrorist organization, or the commission of an offense that is a terrorist act...". "...(b)**One who receives the training or instruction** mentioned in subsection (a) with the intention mentioned in that subsection is liable to seven years' imprisonment...". "...(c)For the

purpose of this section– (1)**It is immaterial whether the training or guidance was given to one person or to a specific or non-specific public**, or whether it was intended for the commission of a specific or nonspecific terrorist act...".

United Kingdom - ***Terrorism Act 2000*** c.11, Part VI, Terrorist Offences, Section 58A **- Eliciting, publishing or communicating information** about members of armed forces etc (1)A person commits an offence who—(a)elicits or attempts to elicit information about an individual who is or has been— (i)a member of Her Majesty's forces, (ii)a member of any of the intelligence services, or (iii)a constable,which is of a kind likely to be useful to a person committing or preparing an act of terrorism, or (b)publishes or communicates any such information....+***Counter-Terrorism and Border Security Act 2019 adds to the Terrorism Act 2000*** following statements : Section 58 of the Terrorism Act 2000 (collection of information) is amended as follows. In subsection (1) (b)after paragraph (b) insert ", or(c)**the person views, or otherwise accesses, by means of the internet a document or record containing information of that kind.**" After subsection (1) insert—"(**1A**)The cases in which a person collects or makes a record for the purposes of subsection (1)(a) include (but are not limited to) those in which the person **does so by means of the internet (whether by downloading the record or otherwise)**. After subsection (3)"It is a defence for a person charged with an offence under this section to prove that he had a reasonable excuse for his action or possession." insert—"(**3A)**The cases in which a person has a reasonable excuse for the purposes of subsection (3) include (but are not limited to) those in which—(a)at the time of the person's action or possession the person **did not know, and had no reason to believe, that the document or record in question contained, or was likely to contain, information of a kind likely to be useful to a person committing or preparing an act of terrorism**, or(b)the person's action or possession was for the purposes of—(i)carrying out work as a journalist, or (ii)academic research."...+***Terrorism Act 2006*** **-** "Section 6 (1) A person commits an offence if— (a) **he provides instruction or training in any of the skills mentioned in subsection** (3); and (b) at the time he **provides the instruction or training**, he knows that a person receiving it intends to use the skills in which he is being instructed or trained—(2) A person commits an offence if— (a) h**e receives instruction or training in any of the skills mentioned in subsection** (3); and (b) at the time of the instruction or training, **he intends to use the skills in which he is being instructed or trained**."

United States - ***U.S Code §2339A*** (Providing material support to terrorists): "...(1) the term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, **training, expert advice** or **assistance**, safehouses, false documentation or identification, **communications equipment**, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials...". +++ ***U.S Code §2339D*** (a) "Whoever knowingly **receives military-type training** from or on behalf of ... a foreign terrorist organization..." (c)(1) "the term "military-type training" includes training in means or methods that can cause death or serious bodily injury, destroy or damage property, or disrupt services to critical infrastructure, or training on the use, storage, production, or **assembly of any explosive, firearm** or other weapon, including any weapon of mass destruction..." - **The Patriot Act (2001) ‘‘**(iv) ENGAGE IN TERRORIST ACTIVITY DEFINED.— (...) the term 'engage in terrorist activity' means, in an individual capacity or as a member of an organization— ‘‘(I) to commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity; "'(II) to prepare or plan a terrorist activity; ‘‘(III) **to gather information on potential targets for terrorist activity; (...)**

European Union - ***Art. 7 Directive (EU)*** 2017/541 "**Providing training for terrorism** - Member States shall take the necessary measures to ensure that **providing instruction** on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the offences listed in points (a) to (i) of Article 3(1), knowing that the skills provided are intended to be used for this purpose, is punishable as a criminal offence when committed intentionally." ***Art 8 Directive (EU)*** 2017/541 "**Receiving training for terrorism** - Member States shall take the necessary measures to ensure that receiving **instruction** on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the offences listed in points (a) to (i) of Article 3(1) is punishable as a criminal offence when committed intentionally.

United Nations - ***Security Council resolution 1267 (1999) :*** "Insists that the Afghan faction known as the Taliban (...) take appropriate effective measures to ensure that the territory under its control is not used for **terrorist installations and camps**, or for the **preparation or organization of terrorist acts** against other States or their citizens"

NATO - ***Brussels Summit Declaration 2018*** : (Point 11) "Building on our Defence Against Terrorism Programme of Work, we will continue to improve our capabilities and technologies (...) to **counter terrorist misuse of technology**".

OSCE - ***Decision 7/06 countering the use of the internet for terrorist purposes*** (2006) : (Point 9) "Tasks the Secretary General to promote, notably through the OSCE Counter-Terrorism Network, the exchange of information on the threat posed by the use of the Internet for terrorist purposes, including incitement, recruitment, fund raising, **training, targeting and planning terrorist acts**, and on legislative and other measures taken to counter this threat".

8. Intelligence

France - ***Code Pénal*** Art.421-2-6 I.2°b) "a) **Recueillir des renseignements** sur des lieux ou des personnes permettant de mener une action dans ces lieux ou de porter atteinte à ces personnes ou exercer une surveillance sur ces lieux ou ces personnes"

Germany - ***German Criminal Code: Section 109f:*** "Whosoever, on behalf of a government agency, a party or another organisation outside the Federal Republic of Germany or for a **banned organisation** or one of its intermediaries 1. collects information about national defence matters; 2. operates an intelligence service dedicated to national defence matters; 3. recruits for or supports one of these activities," + ***German Criminal Code: Section 89a :*** "Whosoever **prepares a serious offence** endangering the state shall be liable to imprisonment." + ***The Network Enforcement Act "NetzDG": Article 1*** "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel - According to Article 25 of the ***Counter-Terrorism Law, 5776-2016 (***25. Providing Resources for Committing a Terrorist Act): "a)One who provides a service or makes resources available to another, as specified below, in circumstances in which doing so may facilitate, directly or indirectly, the commission of an offense that is a terrorist act...". "...(1)**Providing another with** transportation service or a place to sleep, stay or hide, or with **the means to obtain a place to sleep, stay or hide;** (2)**Providing another with** money, food, clothing, **information**, means of communication, documents, vehicles, gasoline, land, a structure, or any other resource...".

United Kingdom – **none.**

United States - ***The Patriot Act (2001) §411 (B) (III) P347***: "to gather information on **potential targets** for terrorist activity..."

European Union – **none.**

United Nations – **none.**

NATO - *(Very General)* ***Brussels Summit Declaration 2018*** : (Point 11) "Building on our Defence Against Terrorism Programme of Work, we will continue to improve our capabilities and technologies (...) to **counter terrorist misuse of technology**".

OSCE - The **OSCE acknowledges** that Member States should take into account different national approaches to defining "illegal" and "objectionable" content and **different methods of dealing with illegal and objectionable content in cyberspace**, such as the possible use of intelligence collected from Internet traffic and content to closing websites of terrorist organizations and their supporters, (…)

9. Communications

France - ***Code Pénal*** Art. 421-2-6 I. 2° c) "**Consulter habituellement un ou plusieurs services de communication au public en ligne** ou détenir des documents provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie".

Germany - ***German Criminal Code Section 89b*** (1) "Whosoever, with the intention of receiving instruction for the purpose of the commission of a serious violent offence endangering the state under section 89a(2) No 1, **establishes or maintains contacts to an organisation within the meaning of section 129a**, also in conjunction with section 129b, shall be liable to imprisonment not exceeding three years or a fine." (129a and 129b are defining terrorist organisations so this is mentioning terrorism). + ***The Network Enforcement Act "NetzDG": Article 1*** "This Act shall apply to telemedia service providers (...) two million registered users in the Federal Republic of Germany (...) sections 86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 241 or 269 of the Criminal Code".

Israel - According to the ***Counter-Terrorism Law, 5776-2016***: (25. Providing Resources for Committing a Terrorist Act): "a)One who **provides a service** or makes resources available to another, as specified below, in circumstances **in which doing so may facilitate**, **directly or indirectly**, the commission of an offense that is a terrorist act...". "...(1)**Providing another** with transportation service or a place to sleep, stay or hide, or **with the means to obtain a place to sleep, stay or hide.** (2)**Providing another with** money, food, clothing, information, **means of communication,** documents, vehicles, gasoline, land, a structure, or any other resource...". +++ ***Prevention of Terrorism Ordinance No. 33 of 5708- (1948), §2***: "A person performing a function in the **management or instruction** of a terrorist organisation or **participating in the deliberations or the framing of the decisions** of a terrorist organisation or acting as a member of tribunal of a terrorist organisation or delivering a propaganda speech a public meeting or over the wireless on behalf of a terrorist organisation shall be guilty of an offence".

United Kingdom - ***Terrorist Act 2006*** - Section 21. Grounds of Proscription: In section 3 of the Terrorism Act 2000 (c. 11) (proscription of organisations), after subsection (5) insert— "(5A) The cases in which an organisation promotes or encourages terrorism for the purposes of subsection (5)(c) include any case in which activities of the organisation— (a) include the unlawful glorification of the commission or preparation (whether in the past, in the future or generally) of acts of terrorism; or (b) are carried out in a manner that ensures that the **organisation is associated with statements containing any such glorification**. - (5C) **In this section— 'statement' includes a communication without words consisting of sounds or images or both."**

United States - ***U.S Code §2339A*** (Providing material support to terrorists): "...(1) the term "material support or resources" means any property, tangible or intangible, or **service**, including currency or monetary instruments or financial securities, financial services, lodging, training, **expert advice or assistance**, safehouses, false documentation or identification, **communications equipment**, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials...".

European Union - ***European Parliament resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations*** : (Point 23) "Raises serious concerns over the increasing use of encryption technologies by terrorist organisations that **make their communications and their radicalisation propaganda impossible** for law enforcement to detect and read, even with a court order; calls on the Commission to urgently address these concerns in its dialogue with internet and IT companies."

United Nations - ***Security Council resolution 2396 (2017) :*** "Noting with concern that terrorists craft distorted narratives, (...) in particular **by exploiting information and communications technologies**, including through the Internet and social media". "Noting with concern that terrorists and terrorist groups continue to use the Internet for terrorist purposes, (...) **prevent terrorists from exploiting technology and communications for terrorist acts**". Point 22."Calls upon member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, **communications** and resources to support terrorist acts".

NATO - ***Brussels Summit Declaration 2018*** : (Point 11) "Building on our Defence Against Terrorism Programme of Work, we will continue to improve our capabilities and technologies (...) to **counter terrorist misuse of technology**".

OSCE - ***DECISION No. 1063 OSCE CONSOLIDATED FRAMEWORK FOR THE FIGHT AGAINST TERRORISM*** ,p.1: "“extradite or prosecute”, any person who supports, facilitates, participates or attempts to participate in the financing, **planning, preparation** or perpetration of terrorist acts or provides safe havens."+++***Resolution on Preventing and Countering Terrorism and Violent Extremism and Radicalization that lead to terrorism*** - "27... stressing the necessity to act cooperatively, including with ICT and social media companies, **to continue to develop and implement practical measures to counter the exploitation of the Internet and other information and communication technologies** for terrorist purposes, including to commit, incite, recruit, fund or plan terrorist acts."

10. Cyberterrorism

France - ***French Penal Code***: 4221-1 (Under the definition of Terrorist Act) "1° wilful attacks on life, wilful attacks on the physical integrity of persons, abduction and unlawful detention and also as the hijacking of planes, vessels or any other means of transport, [...];2° theft, extortion, destruction, **defacement** and damage, and also **computer offences**".

Germany - The German IT Security Act of 2015 deals with **“critical infrastructure”** and its protection from cyberoperations as well as **cyberterrorism**. + ***German Criminal Code Section 303b:*** "Whosoever interferes with data processing operations 3). destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier".

Israel - According to Article 2 of the ***Counter-Terrorism Law, 5776-2016*** (2. Definitions and Interpretation): "a Terrorist Act" is an act that constitutes an offense, or a threat to carry out such an act, which meets all of the following: "...c) **Serious harm**

to property, when in the circumstances in which it was caused there was an actual possibility that it would cause the **serious harm** mentioned in sub-paragraphs (a) or (b) and that was carried out with the intention of causing such harm ; ... e) **Serious harm to infrastructure**, **systems or essential services**, **or their severe disruption**, or serious harm to the State's economy or the environment...". "For the purpose of this definition – "... (b) If the act or threat was carried out using a chemical, biological or radioactive weapon, a harmful substance or a **sensitive facility**, or **while harming a sensitive facility**, where [these weapons or facilities]...". ++ Additionnally, Article Nine ("Damage") of the Israel Penal Law, 5737-1977, subsection 452 on "**Malicious Damage**" indicates that: "If a person **maliciously and unlawfully destroys or damages an asset**, then he is liable to three years imprisonment, and that when no other penalty is prescribed." Subsection 435 on "**Damage in Special Cases**" states that: "If a person commits an offense under section 452 in respect of **a well or bore for water, to a dam, bank, wall or floodgate of a pool or mill pond, or to cultivated trees, to a bridge, water carrier or water reservoir**, then he is liable to five years imprisonment." The Counter-Terrorism Law, 5776-2016 amends subsection 453 of the Penal Law 5737-1977: "(4) In Section 453, the following shall be inserted after subsection (c): (d) Whoever commits an offense as aforesaid in Section 452 **with regard to property that is a sensitive facility** as defined in the Counter-terrorism Law, 5776-2016, is liable to ten years' imprisonment".

United Kingdom - ***Strategies Section 1 of the Terrorism Act 2000 defines*** 'terrorism' as: 1- (2) Action falls within this subsection if it— (a) involves serious violence against a person, (b) **involves serious damage to property** (e) is designed seriously to **interfere with or seriously to disrupt an electronic system**.

United States - According to the ***U.S. Code § 2332b*** - "...(1)Offenses.—Whoever, involving conduct transcending national boundaries and in a circumstance described in subsection (b)—Acts of terrorism transcending national boundaries...". "...(B) creates a substantial risk of serious bodily injury to any other person by **destroying or damaging any structure**, conveyance, or other real or **personal property** within the United States or by **attempting or conspiring to destroy or damage any structure**, conveyance, or other real or personal property within the United States..."; "...***section 1030***(a)(1) (relating to **protection of computers**), ***1030(***a)(5)(A) resulting in damage as defined in

1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers)..." ***section 1362*** (Communication lines, stations or systems): **"...destruction of communication lines, stations, or systems.."; *Section 1992***: **"...terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air..."; *section "2280***a (relating to maritime safety)...". **+ *The Patriot Act (2001)*** - Section 105 - The Director of the United States Secret Service shall take appropriate actions t**o develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model**, throughout the United States, for the p**urpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attack against critical infrastructure and financial payment systems.**

European Union - ***Art. 3 Directive (EU) 2017/541 "Terrorist offences***" states that Member States have the responsibility to "take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences were committed with one of the aims listed in paragraph 2: (d) causing **extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system**, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; +++ ***Art. 21 (EU) Directive 2017/541*** - ***"Measures against public provocation content online*** - 1. Member States shall take the necessary measures to ensure the prompt removal of online content **constituting a public provocation to commit** a terrorist offence, as referred to in Article 5, that is hosted in their territory. They shall also endeavour to obtain the **removal of such content hosted outside their territory.** 2. Member States may, when removal of the content referred to in paragraph 1 at its source is not feasible, take measures to **block access to such content towards the internet users within their territory."**

United Nations - Until now, there is no mutual agreement on issues of terrorism or cyberterrorism, but the ***Draft Comprehensive Convention Against International Terrorism*** prescribes certain criminal offenses that would be considered as acts of terror, including acts that may take place in cyberspace: As in Section 1b & 1c of Article 2 **"Serious damage to public or private property, including a place of public use,**

a State or government facility, a public transportation system, an infrastructure facility or to the environment" (1b) is mentioned as well as "**damage to property, places, facilities or systems (...) resulting or likely to result in major economic loss; when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act"** (1c) which both could be attributed to cyber-attacks on private companies or the Critical National Information Infrastructure. Also, the **UN Global Counter Terrorism Strategy of 2006** was designed to enhance national, regional, and international efforts to counter terrorism in general, including within cyberspace. Additionally, the report on **Countering the Use of the Internet for Terrorist Purposes — "Legal and Technical Aspects of 2011** implemented by the Counter-Terrorism Implementation Task Force" addresses three main subjects: general cybercrime legislation; general counter-terrorism legislation; and Internet-specific counter-terrorism legislation.

NATO - ***NATO's POLICY GUIDELINES ON COUNTER-TERRORISM (2012) (I 1.):*** *Includes cyber in its definition.* "Modern technology increases the potential impact of terrorist attacks employing conventional and unconventional means, particularly as terrorists seek to acquire ... **cyber abilities**." so the following can also relate to cyber: ***NATO's POLICY GUIDELINES ON COUNTER-TERRORISM (2012)(II 5.):*** "Identify key areas in which the Alliance will undertake initiatives to enhance the **prevention of and resilience to acts of terrorism** with a focus on improved awareness of the threat, adequate capabilities to address it and engagement with partner countries and other international actors." + ***Brussels Summit Declaration 2018 : (Point 20) :*** "**Cyber threats** to the security of the Alliance are becoming more frequent, complex, destructive, and coercive. NATO will continue to adapt to the evolving cyber threat landscape, which is affected by both state and **non-state actors,** including state-sponsored." + ***Warsaw Summit Communiqué (2016) (70.):*** Although broad and not terrorism: "Now, in Warsaw, we reaffirm NATO's defensive mandate, and **recognise cyberspace** as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea." + ***Wales Summit (2014) (72.)***: Although broad and doesnt mention terrorism: "Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity,

security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a **cyber-attack would lead to the invocation of Article 5** would be taken by the North Atlantic Council on a case-by-case basis."

OSCE - ***OSCE 2***. Calls on participating States to consider **taking all appropriate measures to protect vital critical information infrastructures and networks against the threat of cyber attacks;** +++ ***Decision No. 1063 OSCE Consolidated Framework for the fight against terrorism*** p.5: "Countering use of the **Internet for terrorist** purposes". *Preventing and countering terrorism and violent extremism and radicalization that lead to terrorism*: 23. **Representative on Freedom of the Media**: Will co-operate in supporting, on request, **the drafting of legislation on the prevention of the abuse of information technology for terrorist purposes**, ensuring that such laws are consistent with commitments regarding freedom of expression and the free flow of information.

Annex 3: Existing Strategies and Policies Regarding Terrorist Use of the Internet

1. Propaganda

France - ***French National Digital Security Strategy (2015)***: "It is the State's responsibility to inform citizens of the risks of manipulation and **propaganda** techniques used by malicious players on the Internet." + Plan National pour la prévention de la radicalisation (Mesure 11 : "Enrayer efficacement **la diffusion de la propagande terroriste** sur internet en accompagnant dans sa mission l'Ambassadeur pour le numérique, chargé de mener un dialogue direct avec les grandes plateformes numériques avec pour objectif prioritaire la mise en place d'outils automatiques d'identification et de retrait afin que les contenus puissent être retirés moins d'une heure après leur mise en ligne.")

Germany - ***The "Cyber Security Strategy for Germany" (2016)*** mentions that **propaganda** or fake news operations conducted by **terrorist** entities might lead to discoursive disruption in Germany in its report on cyber threat assessment of Germany. + ***White Paper on German Security Policy and the Future of the Bundeswehr (2016) (p34.)***: "They use **social media and digital communication** to generate resources, attract supporters, **spread propaganda**, and plan attacks. They increasingly have the ability to attack targets with **cyber capabilities**" "It will ... be necessary to use political, legal, intelligence, police and military resources. Besides hazard prevention, a wide range of additional measures will be necessary in order to successfully deal with the ideological, religious, social and socio-economic causes of radicalisation and **terrorism**."

Israel – **none.**

United Kingdom - ***CONTEST Program*** - Paragraph 91: "We will place a renewed emphasis on our engagement with Communications Service Providers, recognising the internet has been a key way for radicalisers to communicate their propaganda, and for terrorists to plot attacks. We will take robust action to **ensure there are no safe places for terrorists to spread their propaganda online** and to ensure we have the critical access we need to information on their communications. We will build on our

constructive relationship with the tech industry to seek more investment in technologies that automatically identify and remove terrorist content before it is accessible to all, and learn from our work to tackle other illegal and harmful content, such as child sexual exploitation, where we have already made progress." ++ ***CONTEST Programme §111***: "Our response is twofold: working with civil society groups to build their ability to **challenge and counter-terrorist narratives online, and taking robust action to ensure there are no safe places for terrorists online by preventing the dissemination of online terrorist content**."

United States - ***National Strategy for Counterterrorism of the United States of America (2018):*** P22 "Within the United States Government, we will create a common operating picture of **terrorists' propaganda activities to detect and combat terrorists'** narratives and better understand the audiences that they try to influence." +++ **The National Cyber Strategy of the United States of America (2018):** The strategy includes terorism under non-state actors: P2 "Non-state actors— **including terrorists** and criminals — exploited cyberspace to profit, recruit, **propagandize,** and attack the United States ..." Following on from this, the strategy states on P21 "The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and **non-state propaganda** and disinformation."

European Union - ***The European Union Counter-Terrorism Strategy (2005):*** "10. The propogation of particular extermist worldview brings individuals to consider and justify violence. In the context of the most recent wave of terrorism, for example, **the core of the issue is propaganda** which distorts conflicts around the world as a supposed proof of a clash between the West and Islam. To adress these issues, we **need to ensure that voices of mainstream opinion prevail over those of extremism by engaging with civil society and faith groups that reject the ideas put forward by terrorists and extremists that incite violence.** And we need to get our own message across more effectively, to change the perception of national and European policies. We must also ensure that our own policies do not exacerbate division.....+***EU strategic communication to counteract anti-EU propaganda by third parties (2016)*** - 16. calls on the EU and its Member States to develop a counter-narrative to ISIL/Daesh involving the education system and including through **the empowerment and**

increased visibility of mainstream Muslim scholars who have the credibility to delegitimise ISIL/Daesh propaganda; **States to develop and disseminate a counter-narrative to jihadist propaganda, with particular emphasis on an educational dimension demonstrating how the promotion of radical Islam is theologically corrupt**...17. "welcomes the creation of a StratCom Task Force dedicated to the South, which has the potential to contribute effectively to the deconstruction and to the fight against ISIL/ Daesh extremist propaganda and influence."... "20. Calls on the EU and its Member States to take consistent, EU-wide **action against the hate speech being systematically promoted by intolerant, radical preachers through sermons, books, TV shows, the Internet and all other means of communication** that create a fertile ground for terrorist organisations like ISIL/Daesh and Al-Qaeda to thrive"

United Nations - ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to Propaganda, "the importance of protecting an individual's right to freedom of expression has to be balanced with the **need to protect a vulnerable audience from incitement to hatred, discrimination or violence**." +++ ***Uniting against terrorism: recommendations for a global counter-terrorism strategy***: 58. Terrorist networks rely on communication to build support and recruit members. We must deny them this access, particularly by countering their use of the Internet — a rapidly growing vehicle for terrorist recruitment and **dissemination of information and propaganda."**

NATO – **none.**

OSCE – **none.**

2. Psychological Operations

France - ***National Plan for the prevention of radicalisation***: "Prémunir les élèves face au risque de radicalisation dans l'espace numérique et aux **théories du complot** systématisant l'éducation aux médias et à l'information, tout en **développant leur pensée critique et la culture du débat**".

Germany – **none.**

Israel – **none.**

United Kingdom - ***CONTEST Program*** - 95 We will ensure our response reflects our guiding principles of proportionality, flexibility and inclusivity. **Terrorists attack us to create fear, to take revenge** for real and perceived grievances, and to influence public opinion. **We will respond proportionately and in a way that does not undermine our aim to enable people to live freely and with confidence.**

United States – **none.**

European Union – **none.**

United Nations – **none.**

NATO – **none.**

OSCE – **none.**

3. Incitement

France - ***National Plan for the prevention of radicalisation*** : "**Enrayer efficacement** la diffusion de la propagande terroriste sur internet en accompagnant dans sa mission l'Ambassadeur pour le numérique, chargé de mener un dialogue direct avec les grandes plateformes numériques avec pour objectif prioritaire la mise en place d'**outils automatiques d'identification et de retrait** afin que les contenus puissent être retirés moins d'une heure après leur mise en ligne" (a bit debatable, same as propaganda)

Germany – **none.**

Israel – **none.**

United Kingdom - ***CONTEST program:*** "11.We will share information more widely and support more local interventions with individuals in our own communities **who are**

being groomed or incited to commit or support acts of terrorism. 89 We will share information more widely and **support more local interventions with individuals in communities being groomed or incited to commit or support acts of terrorism**.

United States - ***National Strategy for Counterterrorism of the United States of America (2018)***: P22 "We will combat terrorist use of cyberspace as a global stage to showcase their violent ideologies, to fundraise, and to radicalize, recruit, and **mobilize individuals to violence."**

European Union - ***The European Union Counter-Terrorism Strategy (2005)*** - "13. Key priorities for 'Prevent' are to : **Address incitement and recruitment** in particular key environments as prisons, places of religious training or worship, notably **by implementing legislation making these behaviors offences."**

United Nations - ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to Propaganda, "the importance of protecting an individual's right to freedom of expression has to be balanced with the need to protect a vulnerable audience **from incitement to hatred, discrimination or violence."**

NATO – **none.**

OSCE – **none.**

4. Recruitment

France - ***French Digital Security Strategy (2015)*** - "...groups of individuals with diverse motivations and supports, **mercenaries recruited worldwide and associated** according to the circumstances, regularly take recourse in cyberattacks to attempt to destabilise the governing authorities of many countries or businesses that symbolise them. In addition, **terrorist organisations take advantage of the audience provided by social networks to disseminate propaganda intended to attract volunteers and terrorise the populations**. These different groups benefit from continuous media impact.

Germany - ***White Paper on German Security Policy and the Future of the Bundeswehr (2016) (p34.)***: "They use s**ocial media and digital communication** to generate resources, **attract supporters**, spread propaganda, and plan attacks. They increasingly have the ability to attack targets with **cyber capabilities**" "It will ... be necessary to use political, legal, intelligence, police and military resources. Besides hazard prevention, a wide range of additional measures will be necessary in order to successfully deal with the ideological, religious, social and socio-economic causes of radicalisation and **terrorism.**"

Israel – **none.**

United Kingdom - ***CONTEST programme*** - "114 We introduced the Prevent statutory duty through the Counter-Terrorism and Security Act 2015. The duty requires local authorities, schools, colleges, higher education institutions, health bodies, prisons and probation, and the police to consider the need **to safeguard people from being drawn into terrorism.** The duty is designed to help ensure that vulnerable individuals who are at risk of radicalisation are supported as they would be under other safeguarding processes."

United States - ***National Strategy for Counterterrorism of the United States of America (2018)****:* P21 "To undercut terrorist recruiting, we will demonstrate that their claims are false and do not offer effective solutions. We will exploit doubts among potential recruits to **reduce terrorists' ability to incite violence and recruit.** We will also communicate alternatives and promote off ramps from violence to prevent individuals from becoming more committed to these ideologies and their violent means. Throughout this cycle of recruitment and mobilization, we will take advantage of our operational, diplomatic, and development successes to demonstrate the futility of terrorist violence....+(Pg. 14.) This message will aim to **discredit terrorist narratives, dissuade potential terrorist supporter**s, and demonstrate that the effects of our counterterrorism operations are not limited solely to direct action. +++ **National Security Strategy of the United States of America (2017)**: P11 "We will degrade their ability to message and attract **potential recruits**."

European Union - ***Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism (2014)***: "27. **We should support and amplify counter narratives emanating** from those with local influence, including community leaders where this concept applies, who lead or shape public opinion and who can tell a positive and credible story. **We should initiate projects with these actors at all levels and work to ensure that they are appropriately empowered and supported**....31. **Work to counter online radicalisation and recruitment to terrorism** is wide-ranging. It covers activities aimed **at disrupting terrorist use of the internet, but also initiatives to challenge the terrorist narrative**. Some of it can be done at national or European level and some of it by people and organisations from within civil society, facilitated where necessary.

United Nations - ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to Recruitment, " Doing so must also acknowledge the **important role and needs of women and girls, who are increasingly bearing the brunt of terrorist acts and being radicalized and recruited by terrorist groups. Equally important to prevention is the need to focus on young people**. Effective action in this area would entail a renewed focus on conflict prevention and resolution; fostering dialogue, understanding and social inclusion; equitable and just socioeconomic development; and promoting the positive role that women and young people can play in society."...+***UN Global Counter-Terrorism Strategy (2006***) - "6.To pursue and reinforce development and social inclusion agendas at every level as goals in themselves, recognizing that success in this area, especially on youth unemployment, **could reduce marginalization and the subsequent sense of victimization that propels extremism and the recruitment of terrorists."**

NATO – none.

OSCE – none.

5. Radicalization

France - ***Plan National pour la prevention de la radicalisation*** (National Plan for the prevention of radicalisation - 2018) **+** ***French National Digital Secuity Strategy (2015)***: "After the terrorist attacks against France in January 2015, the Government established an information platform on the risks related to Islamic radicalisation via the electronic communication networks : « **Stop-djihadisme.gouv.fr** ».

Germany - ***BAMF's 'Advice Centre on Radicalisation***' was established by the ' Federal Office for Migration and Refugees on 1 January 2012.' It supports those whose friends and/or family has been radicalized. If they suspect a family member or friend is becoming radicalized they first phone BAMF who will provide assistance on what to do next and aim to get them 'out of the spiral of radicalisation'. For example, 'establish direct contact with specialists.' + ***White Paper on German Security Policy and the Future of the Bundeswehr (2016)(p34.):*** "Besides hazard prevention, a wide range of additional measures will be necessary in order to successfully deal with the ideological, religious, social and socio-economic causes of **radicalisation and terrorism**. Radical thinking and behaviour must also be countered at home."

Israel – **none.**

United Kingdom - ***CONTEST programme*** paragraph 13: "We will prioritise **strengthening the resilience of local communities to terrorism** as they are at the forefront of our response, in particular those **where the threat from terrorism and radicalisation is highest**." Paragraph 16: "To **safeguard and support those vulnerable to radicalisation**, to stop them from becoming terrorists or supporting terrorism, we will: Focus our activity and resources in those locations where the threat from terrorism and radicalisation is highest. Focus our online activity on **preventing the dissemination of terrorist material and building strong counter-terrorist narratives** in order to ensure there are no safe places for terrorists online. Re-enforce safeguarding at the heart of Prevent **to ensure our communities and families are not exploited or groomed into following a path of violent extremism.**" + ***CONTEST Programme*** §124: "If an individual is assessed to be **vulnerable to radicalisation**, they may be offered support through the Channel programme in England and Wales, or the Prevent Professional Concerns (PPC) programme in Scotland. These are multi-agency

programmes **designed to safeguard and support vulnerable individuals at risks of being drawn into terrorism**."

United States - ***National Strategy for Counterterrorism of the United States of America (2018)***:P22 " We will identify signs of violent **radicalization and mobilization to focus real-world and online intervention** efforts to prevent terrorist attacks... We will co**mbat terrorist use of cyberspace as a global stageto showcase their violent ideologies, to fundraise, and to radicalize, recruit, and mobilize individuals to violence.** In concert with our partners, we will expand relationships with technology sector entities **to empower them to combat violent extremism online and terrorists' abuse of their platforms.** We will continue to expose and counter the flood of terrorist ideology online. +++ **National Security Strategy of the United States of America (2017)**: This strategy accknowledegs the use of the internet stating: P10 "**Jihadist terrorists use virtual** and physical networks around the world to radicalize isolated individuals..." Following on from this the action it recommends is: P11 "U.S. intelligence and homeland security experts will work with law enforcement and civic leaders on terrorism prevention and provide accurate and actionable information about **radicalization** in their communities."

European Union - ***Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism (2014)***: .31. **Work to counter online radicalisation** and recruitment to terrorism is wide-ranging. It covers activities aimed at disrupting terrorist use of the internet, but also initiatives to challenge the terrorist narrative. Some of it can be done at national or European level and some of it by people and organisations from within civil society, facilitated where necessary.

United Nations - ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to Radicalization, "61. Terrorists have cleverly exploited new communications technologies to radicalize and recruit young people around the world, and there is a significant risk that they could launch cyberterrorism with devastating effect in the coming years. **This demonstrates the need for increased international cooperation to counter Internet radicalization and recruitment,** but it must be done in a manner that ensures and promotes freedom of expression and upholds international human

rights norms and standards." +++ ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** includes several former and ongoing programs and activities to counter violent extremism and radicalization. For instance UNICRI (United Nations Interregional Crime and Justice Research Institute) has been working in the area of de-radicalisation of prisoners and is developing re-entry programming for such prisoners, as well as for returning Foreign Terrorist Fighters. UNICRI also recently launched a four-year programme to counter radicalisation and violent extremism in the Sahel Maghreb region. The focus of this program lies on the implementation through civil society and non-state actors and the promotion of crossborder cooperation. Additionally, the UNCCT (United Nations Counter-Terrorism Centre) has established a rapidly deployable List of Counter-Terrorism Advisors to support Member States on four key thematic areas: developing counterterrorism strategies, countering radicalisation, vulnerable targets and victims support. Ongoing projects also include the project of "Assisting Horn and Eastern Africa countries to Strengthen Rule of Law based Criminal Justice Responses to Terrorism and Violent Extremism" conducted by the UNODC (United Nations Office on Crime) which focuses on addressing legal and criminal justice aspects of radicalization, violent extremism and foreign terrorist fighters; cross-border judicial cooperation; adopting/revising counter-terrorism legal frameworks. Another ongoing project by the UNODC includes the "UNODC Handbook on the Management of Violent Extremist Prisoners (VEPs) and the Prevention of Radicalisation to Violence in Prisons" - "a comprehensive publication to provide practical guidance to prison administrators and policy makers; two international Expert Group Meetings." The UN Counter-Terrorism Committee (CTC) - together with the European Union and the United Nations Office on Crime (UNDOC) provides technical assistance on the management of VEPs and the prevention of radicalisation to violence in prison in the Middle East and North Africa.

NATO – **none.**

OSCE – **none.**

6. Financing

France - ***Plan d'action national contre le financement du terrorisme*** **(2015)** : "Améliorer la **traçabilité** des opérations financières en réduisant l'anonymat des transactions, mobiliser les acteurs financiers et renforcer les capacités de **gel des avoirs** des financeurs et des acteurs du terrorisme."

Germany – **none.**

Israel – **none.**

United Kingdom - ***CONTEST Programme*** §153: " We will continue to **act against fundraising for terrorist organisations and terrorist financing, including by freezing terrorists' assets**, working closely with the finance sector."

United States - ***National Strategy for Counterterrorism of the United States of America (2018):*** P16 "We will ... enhance information-sharing regarding terrorists' financial data, transactions, and activities. We will use this information ... to **deny terrorists the ability to raise funds**, including by disrupting terrorist financing and dismantling terrorist support networks, to prevent terrorists from abusing the United States and global financial systems, and to dissuade people from providing funds or materiel to terrorists." +++ **U.S. Department of Homeland Security Cybersecurity Strategy (2018)**: Does not specifically mention financing terror but: "DHS must continue to focus on our core investigative responsibilities **regarding financial services and payment systems** ... misuse of cryptocurrencies, and other violations of customs law through the Internet or online marketplaces." +++ **National Security Strategy of the United States of America (2017)**:P11 "We will disrupt the financial, materiel, and personnel supply chains of terrorist organizations. We will **sever their financing** and protect the U.S. and international financial systems from abuse."

European Union - ***The European Union Counter-Terrorism Strategy (2005)***: "29. Creating a hostile operating environment for terrorists also means **tackling terrorist financing**. The EU has already put in place provisions for **freezing assets.** The next stage is to implement the EU-wide legislation concerning **money laundering and cash transfers, and to agree steps to impede money (wire) transfers by terrorists.** In

addition, tackling the **misuse of the non-profit sector** remains a priority. We must also ensure that financial investigation is an integral part of all terrorism investigations."

United Nations - The UN's main global instrument in combating terrorism - ***the Global Counter Terrorism Strategy, adopted in 2006***, mentions that UN member states should "**refrain from organizing, instigating, facilitating, participating in, financing, encouraging or tolerating terrorist activities** and to take appropriate practical measures to ensure that our respective territories are not used for terrorist installations or training camps, or for the preparation or organization of terrorist acts intended to be committed against other States or their citizens." +++***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to The UNCCT also launched a project on 'International Good Practices on Addressing and Preventing Kidnapping for Ransom (KFR)' **which seeks to contribute to curbing the ability of terrorist organizations to raise funds through KFR**. The Centre is also supporting a UNODC implemented project on 'Mock Trials on Financing of Terrorism' which seeks strengthen capacity of criminal justice officials in Argentina and Colombia **to counter the financing of terrorism.**

NATO - ***Partnership Action Plan Against Terrorism (2002) (16.3.2):*** "EAPC States will exchange information and views in the EAPC Economic Committee on the economic aspects of the international fight against terrorism, in particular on regulatory provisions **barring the financing of terrorist activity** and methods and sources of finance for terrorist groups.

OSCE – **none.**

7. Information Sharing

France – **none.**

Germany - ***White Paper on German Security Policy and the Future of the Bundeswehr (2016) (p34.):*** "They use social media and **digital communication** to

generate resources, attract supporters, spread propaganda, and **plan attacks.** They increasingly have the ability to attack targets with cyber capabilities" "It will ... be necessary to use political, legal, intelligence, police and military resources. Besides hazard prevention, a wide range of additional measures will be necessary in order to successfully deal with the ideological, religious, social and socio-economic causes of radicalisation and **terrorism.**"

Israel – **none.**

United Kingdom - ***CONTEST programme*** - "49. Daesh's media and propaganda capability has been significantly degraded. But its shift to a narrative of victimhood and seeking to weaponise people in their communities, rather than encouraging them to travel to the "Caliphate", has led to a self-sustaining network of Daesh supporters who create and share unofficial motivational and **instructional material online**, and celebrate and encourage lone actor attacks. "

United States - ***U.S. Department of Homeland Security Cybersecurity Strategy (2018)***: Doesnt specifically mention terrorists but: P17 "DHS must better align our existing law enforcement efforts and resources to address new and emerging challenges in cyberspace, to include the **growing use of end-to-end encryption**, anonymous networks, online marketplaces, and cryptocurrencies." +++ **National Security Strategy of the United States of America (2017)**: P11 "We will ... confront the challenge of terrorists and criminals "going dark" and using secure platforms to evade detection."+ ***National Strategy for Counterterrorism of the United States of America (2018)*** - "We will **prevent terrorists from developing or acquiring knowledge and material that enables the development of WMD and other advanced weapons**, including the capability to perform large-scale cyber attacks. We will work with partner nations, international organizations, and commercial entities to improve their capacity to secure dangerous materials and **ensure that terrorists cannot exploit the scientific and academic communities to acquire new capabilities."**

European Union - ***The European Union Counter-Terrorism Strategy (2005)*** - "28. Terrorists must also be deprived of the means by which they mount attacks - whether directly (eg **weapons and explosives**) or indirectly (eg f**alse documentation to enable**

undetected travel and residence). Their **ability to communicate and plan undetected should be impeded** by measures such as the retention of telecommunication. They must also be deprived as far as possible of the opportunities offered by the Internet to communicate and spread technical expertise related to terrorism."+++***Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism (2014)*** **-** 30.The internet and social media can be used for the dissemination of propaganda material, fundraising, recruitment and communication with like-minded individuals, **but also as a virtual training camp, as well as a means of exchanging skills and know-how**. The internet is also a transnational entity transgressing various national jurisdictions.

United Nations – **none.**

NATO – **none.**

OSCE – **none.**

8. Intelligence

France ***- Defence and national security strategic review (2017)*** : "Today's jihadist organisations - Daesh, Al-Qaeda and their various affiliates - stand as an ideological and operational matrix, passing on their **expertise** from generation to generation, and have demonstrated an **ability to adapt and mutate** despite suffering setbacks . Branches of these networks thrive on chaos, civil war and ungoverned regions and put down roots in new areas, aided by the **return or transfer of experienced** leadership from combat zones in the Middle East"

Germany – **none.**

Israel – **none.**

United Kingdom ***- CONTEST programme*** **-** "78. Evolving technology creates new challenges, risks and opportunities in fighting terrorism. Terrorists use new

technologies, **like digital communications and unmanned aerial vehicles, to plan and execute attacks**, and tend to adopt them at the same pace as society as a whole. +284 Daesh used its control of territory in Syria and Iraq to **train operatives, plan and execute attacks**, seize resources, launch propaganda campaigns and exploit and abuse local populations. A key part of our overall approach is **proactively degrading and weakening such key terrorist structures and enablers which help drive the direct threat to us**. In order to protect UK citizens at home and abroad, we are continuing to play a leading part in a Global Coalition of 75 members to defeat Daesh in Syria and Iraq.

United States – **none.**

European Union - ***The European Union Counter-Terrorism Strategy (2005)*** - "28. Terrorists must also be deprived of the means by which they mount attacks (...). Their ability to communicate and **plan undetected** should be impeded by measures such as the retention of telecommunication. They must also **be deprived as far as possible of the opportunities offered by the Internet to communicate and spread technical expertise related to terrorism**."

United Nations – **none.**

NATO – **none.**

OSCE – **none.**

9. Communications

France – **none.**

Germany - ***White Paper on German Security Policy and the Future of the Bundeswehr (2016) (p34.)***: "They use social media and **digital communication** to generate resources, attract supporters, spread propaganda, and plan attacks. They increasingly have the ability to attack targets with cyber capabilities" "It will ... be

necessary to use political, legal, intelligence, police and military resources. Besides hazard prevention, a wide range of additional measures will be necessary in order to successfully deal with the ideological, religious, social and socio-economic causes of radicalisation and **terrorism**."

Israel – **none.**

United Kingdom - ***CONTEST programme*** paragraph 12: "...We will jointly with industry improve security at venues in the UK, gain faster alerts to suspicious purchases and design out vulnerabilities in our infrastructure or in products that terrorists exploit. We will take robust action to ensure there are no safe places for terrorists online, and **ensure we have the critical access we need to information on their communications.** We will seek more investment in technologies that automatically identify and remove terrorist content before it is accessible to all.." + ***CONTEST Programme*** §143: "We and the police and the security and intelligence agencies will continue to **develop capabilities to ensure we can collect and analyse terrorist communications and their use of digital media** in order to detect threats. This investment will be done in partnership and in accordance with the requirements of the Investigatory Powers Act 2016 for acquiring, holding and using such information. "

United States - ***U.S. Department of Homeland Security Cybersecurity Strategy (2018)***: Doesnt specifically mention terrorists but: P17 "DHS must better align our existing law enforcement efforts and resources to address new and emerging challenges in cyberspace, to include the **growing use of end-to-end encryption**, anonymous networks, online marketplaces, and cryptocurrencies." +++ **National Security Strategy of the United States of America (2017)**: P11 "We will ... confront the challenge of terrorists and criminals “going dark” and using secure platforms to evade detection."

European Union - ***The European Union Counter-Terrorism Strategy (2005)*** - "28. Terrorists must also be deprived of the means by which they mount attacks - whether directly (eg weapons and explosives) or indirectly (eg false documentation to enable undetected travel and residence). T**heir ability to communicate and plan undetected should be impeded by measures such as the retention of telecommunication.** They

must also be **deprived as far as possible of the opportunities offered by the Internet to communicate and spread technical expertise related to terrorism.**"

United Nations - ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to Communication INTERPOL is developing a proactive SOCMINT (Social Media Intelligence) program, with both analytical and operational components, to support member countries to address the challenges and opportunities created by **increasing use of internet and other information tools by terrorist groups such as ISIL. ++** ***Uniting against terrorism: recommendations for a global counter-terrorism strategy (2006)*** -Terrorist networks rely on communication to build support and recruit members. **We must deny them this access, particularly by countering their use of the Internet** — a rapidly growing vehicle for terrorist recruitment and dissemination of information and propaganda.

NATO – **none.**
OSCE – **none.**

10. Cyberterrorism

France - ***French National Digital Security Strategy (2015):*** "France will continue to reinforce the security of its critical networks and its resilience in case of a major **cyberattack** by expanding cooperation with private stakeholders at national and international levels.+ The role of the State i**n cyberspace is to ensure France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyberattack** (objective 1), to protect the digital lives of citizens and businesses and **combat cybercriminality** (objective 2), to ensure the education and **training required for digital security** (objective 3), to contribute to the development of an environment that is conducive to **trust in digital technology** (objective 4) and to promote cooperation between Member States of the European Union (EU) in a manner favourable to the emergenceof a European **digital strategic autonomy, a long-term guarantor of a cyberspace** that is more secure and respectful of our values (objective 5). " **+** ***French White Paper: Defense and National Security***

(2013): "Cyberspace has thus become an area of confrontation as such. The possibility - envisaged by the previous White Paper - of a major **cyber-attack** on national information systems in a scenario of cyber warfare constitutes an extremely serious threat for France and its European partners."+++***Defence and national security strategic review (2017***) The **Internet-related** service companies that have arisen from the digital revolution, such as **Google, Facebook, and Baidu, must now be considered as major stakeholders in the geopolitical environment**. Their vast user bases enable them to collect and monitor huge volumes of data, and to provide essential services.These platforms **have become critical to counter-terrorism, cybersecurity, personal data protection and, in some cases, cyberattack detection, attribution, and response.**

Germany - ***White Paper on German Security Policy and the Future of the Bundeswehr (2016) (p36.):*** Defines using terrorism in its definition of cyber attack: "Access to destructive malware is relatively easy and inexpensive. As a result, the means to carry out cyber attacks are not restricted to state actors. **Terrorist groups** ... can potentially cause serious damage with minimal effort" + ***White Paper on German Security Policy and the Future of the Bundeswehr (2016) (p38.):*** Thus the recommendations can relate to cyber terror: "Besides working on a common understanding of the application of international law, we must also improve our **responsiveness and resilience as well as our capability to prevent and defend against cyber attacks** and information operations. This includes coherent and coordinated strategies in NATO and the EU."

Israel - ***Government Resolution No. 2444 of February 15, 2015*** - "A National Cyber Security Authority 2.a :To **conduct, operate and implement, as needed, all the operational defensive efforts in cyberspace at the national level, from a holistic perspective, for the purpose of providing a complete and continuous defensive response to cyber attacks**, including handling cyber threats and incidents in real time, formulating an ongoing situational awareness, consolidating and analyzing intelligence, and working with the defense community.... National activity for cyber security 5: **To charge the Bureau with the task of establishing in the Authority a national technological and organizational infrastructure for early warning, analysis, alert**

and sharing of information, in order to expose and identify cyber attacks on the State of Israel."

United Kingdom - ***National Cyber Security Strategy 2016-2021***: 2.3. "Malicious actors – hostile states, criminal or terrorist organisations and individuals – can exploit the gap between convenience and security. Narrowing that gap is a national priority. 4.16. The intelligence agencies, the Ministry of Defence, the police and the National Crime Agency, in coordination with international partner agencies, will **expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists.** "

United States - ***National Strategy for Counterterrorism of the United States of America (2018)***: P16 " We will prevent terrorists from developing or acquiring knowledge and material that enables the development of WMD and other advanced weapons, including the capability to perform **large-scale cyber attacks**." +++ **U.S. Department of Homeland Security Cybersecurity Strategy (2018)**: P16 "working with national and international partners through electronic crimes task forces to prevent, detect, and investigate various **cyber crimes, including potential terrorist attacks** against critical infrastructure and financial payment systems, as well as improving the security of federal facilities." +++ **National Security Strategy of the United States of America (2017)**: P13 "The Federal Government will ensure that those charged with securing critical infrastructure have the necessary authorities, information, and capabilities to prevent attacks before they affect or hold at risk U.S. critical infrastructure. The United States will impose swift and costly consequences on foreign governments, criminals, and **other actors** who undertake significant malicious cyber activities. " +++ **The National Cyber Strategy of the United States of America (2018)**: P11 "The United States should also aid willing partner nations to build their capacity to address criminal cyber activity. The borderless nature of cybercrime, including ... **terrorist activities,** requires strong international law enforcement partnerships. This cooperation requires foreign law enforcement agencies ... to assist United States law enforcement ..."

European Union - ***The European Union Counter-Terrorism Strategy (2005)*** - "18. **Reducing the vulnerability across Europe of critical infrastructure to physical and**

electronic attack is essential. To further encance our protection, we agreed to establish a Programme of work aimed at improving the protection of critical infrastructure across Europe. We will continue work to this end, developing an all hazard approach which recognises the threat from terrorism as priority."

United Nations - ***Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (2016)*** states that with regards to Cyberterrorism, "61. A related **focus must be on preventing acts of cyberterrorism** by individuals associated with violent extremism and terrorism. **Modern electronic communications networks provide the backbone to the most critical infrastructure**, including the essential functions of Government and industry. Safeguarding this infrastructure from cyberterrorism cannot succeed without stronger partnerships with the private sector.

NATO - ***The Alliance Strategic Concept (2010*) *(12.)*** includes terrorism as a cuase of cyber attacks: "**Cyber attacks** are becoming more frequent, more organised and more costly in the damage that they inflict ... **terrorist and/or extremist groups** can each be the source of such attacks." + T***he Alliance Strategic Concept (2010) (19.):*** "develop further our ability to **prevent, detect, defend against and recover from cyber-attacks**, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations".

OSCE – **none.**

END