Democracy and Security

ISSN: 1741-9166 (Print) 1555-5860 (Online) Journal homepage: https://www.tandfonline.com/loi/fdas20

The War on Cyberterrorism

Marco Marsili

To cite this article: Marco Marsili (2019) The War on Cyberterrorism, Democracy and Security, 15:2, 172-199, DOI: 10.1080/17419166.2018.1496826

To link to this article: https://doi.org/10.1080/17419166.2018.1496826

DEMOCRACY AND SECURITY
2019, VOL. 15, NO. 2, 172–199
https://doi.org/10.1080/17419166.2018.1496826

Routledge
Taylor & Francis Group

The War on Cyberterrorism

Marco Marsili

Centro de Estudos Internacionais (CEI-IUL), Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal; Centro de Investigação, Inovação e Desenvolvimento da Academia Militar (CINAMIL), Lisboa, Portugal

ABSTRACT

This article addresses the problem of international law enforcement within the War on Cyberterrorism. Hybrid conflicts have replaced the traditional ones, and new threats have emerged in cyberspace, which has become a virtual battlefield. Cyber threats - cybercrimes, cyberterrorism, cyberwarfare - are a major concern for Western governments, especially for the United States and the North Atlantic Treaty Organization. The international community has begun to consider cyberattacks as a form of terrorism, to which the same measures apply. Because the term "terrorism" is ambiguous and legaly undefined, there is no consensus on a definition of the derivative term "cyberterrorism", which is left to the unilateral interpretations of states. Pretending to consider the cyberspace domain as traditional domains, and claiming to apply IHL for the sole purpose of lawfully using armed forces in contrast to cyberterrorism is a stretch. This paper addresses the question of whether or not current laws of war and international humanitarian law apply to cyber domain, and gives some recommendations on how to tackle this issue.

KEYWORDS

Cyberterrorism; cybersecurity; cyberdefense; cyberspace; cybercrime

Defining Cyberterrorism

So far, it has not been possible to reach an undisputed definition of terrorism due to major divergences on the legitimacy of the use of violence for political purposes.[1] The term is ambiguous and undefined, and at present there is no commonly accepted definition,[2] either legal nor academic. The definition of "terrorism" is left to the unilateral interpretations of states,[3] and it easily falls prey to change that suits the interests of particular states at particular times.[4] Consequently, there is no consensus on a legal or academic definition of the derivative term "cyberterrorism," which was introduced by Barry Collin in 1997.[5] As for terrorism, there is debate over the basic definition of the scope of cyberterrorism, depending on motivation, targets, methods, and centrality of computer use in the act.

Cyberspace involves both military and civilian security, as governments rely on the Internet and telecommunication systems for a wide range of

CONTACT Marco Marsili marco_marsili@iscte-iul.pt; info@marcomarsili.it Centro de Estudos Internacionais (CEI-IUL), Instituto Universitário de Lisboa (ISCTE-IUL), Av. das Forças Armadas, Lisboa 1649-026, Portugal.

critical services.[6] Security is a broad-scope concept, which involves the protection of the state and its citizens. Cybersecurity deals with the protection of computer systems from theft, damage, or disruption.[7] Cybercriminals fall into the provisions of criminal law on cybercrime and should be prosecuted under these rules. Law enforcement agencies face cybercrime just as they deal with terrorism. The boundary between crime and terrorism is thin, and these offenses need an adequate setting.

According to the Federal Bureau of Investigation (FBI), cyberterrorism is "[any] premeditated, politically motivated attack against information, computer systems or computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents." The North Atlantic Treaty Organization (NATO) characterizes it as "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."[8]

We can choose a very narrow definition of cyberterrorism, relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption, or a broader definition, which includes cybercrime. Matusitz[9] provides a broader definition of cyberterrorism, which includes the intentional use of computers, networks, and public Internet to cause destruction and harm for personal objectives.

Participating in a cyberattack affects the terror threat perception, even if it is not done with a violent approach.[10] By some definitions, it might be difficult to distinguish which instances of online activities are cyberterrorism or cybercrime.[11] Cyberterrorism may overlap considerably with cybercrime, cyberwar, or ordinary terrorism. However, when it is done for economic motivations rather than ideological, it is typically regarded as cybercrime.[12] Some scholars have deepened these ties. Erbschloe[13] explores the connections of information warfare between economy and national defense. Conway[14] wonders whether terrorist groups who operate in cyberspace are "cyberterrorists." She concludes that the answer hinges on what constitutes cyberterrorism, considering that terrorism is a notoriously difficult concept to define. What is the difference between terrorism and common crime? This distinction is crucial to determine under what rules fall the perpetrators of cyberattacks.

The first distinctive character of terrorism is the instillation of fear. The second distinctive sign is the use of violence or the threat of violence. There can be no terrorism without the use of force, but violence is also one of the general characteristics of criminal acts. The third distinctive sign of terrorism is the political motivation or political purpose. An action that instills terror cannot automatically be regarded as terrorism. Without

political motivation or political purpose, a cyberattack cannot be considered a terrorist attack but must be characterized as a common crime.

Klabbers believes that the terrorist is usually "politically inspired" and has an interest in being seen so, whereas for the state it is tempting to treat him as a common criminal.[15] Morgan thinks that terrorism is both crime and politics and is culpable on both accounts,[16] while Khan argues that the political dimension of terrorism differentiates it from other crimes.[17] Hoffman affirms that terrorism is just a form of crime,[18] and Schmid simply suggests treating acts of terrorism as "peacetime equivalents of war crimes."[19] Klaber infers that due to the problem of containing terrorism within regular categories of criminal law, a way to treat terrorists is to consider them simply as common criminals.[20] He gathers that even though international law has great difficulty in deciding whether terrorists should be treated as ordinary criminals or as political actors, the limit for governments that may lawfully characterize them as criminals is extremely flexible. Pictet concludes that governments tend to consider non-state actors as common criminals[21] just not to apply the provisions of Article 3 of the Geneva Conventions of 1949.[22]

Meisels believes that whereas irregular combatants, such as terrorists or insurgents, are not entitled to the protection accorded by the law of war, they do not enjoy the rights granted to criminals in civil law due to their hybrid identity.[23] She considers that the combatant-civilian hybrid identity does not constitute a prosecutable offense in itself, but that specific acts of war can be deemed war crimes, perhaps as terrorism.[24] Meisels points out that international law and practice leave irregular combatants unprotected, even if their unlawful identity is not in itself a criminal offense.[25] Brants concludes that criminal categories are better to be applied to individuals, rather than to groups.[26]

The term "terrorism" is still ambiguous and undefined due to the contradictory ideologies of the states.[27] Bassiouni[28] briefly concludes that "'[t]errorism' has never been defined." Rosalyn Higgins, former judge at the International Court of Justice, considers that "[t]errorism is a term without legal significance."[29] She deduces that "it is merely a convenient way of alluding to activities, whether of states or of individuals, widely disapproved of and in which either the methods used are unlawful, or the target protected or both."[30] Klabbers argues that the language of terrorism in necessary to justify a large-scale response.[31] Saul thinks that criminalizing terrorism is only a small part of the overall international response.[32]

Grove[33] acknowledges that responding to cyberdefense raises legal questions. He concludes that international customary law is not yet fully formed on this issue, but the UN Charter and the laws of armed conflict establish certain baseline rules.

In my opinion the problem lies in international customary law. I think that the customary law that is being formed recently is contrary to the principles established by international humanitarian law, which is binding for all states.

Approaching Cyberterrorism

Many authors have documented that cyberterrorism is a real threat that must be seriously addressed. Valeri and Knights[34] stress the ties between terrorism and information warfare, which target elements of the critical national information infrastructure. Shimeall[35] argues that defense planning has to incorporate the virtual world to limit physical damage in the real. Brickey[36] and Heffelfinger[37] provide us with evidence of acts of jihadist cyberterrorism carried out between 2008 and 2012, and they acknowledge the risks posed by Islamist hacking activity.

Yet in 2001, Arquilla and Rondfeldt, in their seminal work *Networks and Netwars*, include the term "netwar" in a list of "trendy synonyms."[38] At a first stage, scholars took into account propaganda and online recruitment through social media, even if they considered it a serious threat. In *Terrorism in Cyberspace*, Gabriel Weimann states that the War on Terror (WoT) has not been won, as it continues on in the cyberdomain.[39] Weimann emphasizes the use of the Web and social media for propaganda and recruitment purposes.

Blunt's approach to the issue is different and more complete. In his seminal work, the specialist writer and researcher on Islam, Muslims, and cyberspace encompasses the hacking and cracking (infiltration and sabotage, respectively) of "enemy" computer systems, which can result in "e-mail overload, system failure, the defacement of web content, database acquisition and dysfunctional and crashed sites"[40] According to Blunt, cyberterrorism is a real threat to US security and should be addressed seriously.[41]

Awan and Blakemore approach cyberterrorism in a multidisciplinary and comprehensive way, encompassing criminology, security studies, social policy, and Internet law. In *Policing Cyber Hate, Cyber Threats, and Cyber Terrorism*, the authors deal with cybercrime, terrorism, policing cyberspace, cyber hate, and government strategies.[42] This book provides a comprehensive understanding of the range of activities that can be defined as cyber threats, from cybercrimes to online terrorism. The editors stress the importance of countering the cyber threat, which presents a clear and present danger.

Holt, Burruss, and Bossler analyze the responses of US law enforcement agencies at all levels in dealing with cybercrime and cyberterror.[43] The findings demonstrate the realities of policing cybercrimes and those involving digital evidence processing relative to traditional offenses. *Policing Cybercrime and Cyberterror* suggests policy changes needed to increase the investigative response of police agencies.

Jarvis, MacDonald, and Chen offer a holistic approach to cyberterrorism, including law, politics, technology, and beyond.[44] Their book *Terrorism Online* uses a multidisciplinary framework to provide a broader analysis of the topic, and it explores different forms of terrorism, including hacktivists and state-based terrorism. The discussion on the role of NATO is especially mentionable in this context.[45]

In 2008 NATO opened a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn,[46] the capital of Estonia, which had joined the Alliance four years before. In April 2007 the Baltic state was targeted by a massive cyberattack that ultimately rendered the country offline and shut out from services dependent on Internet. Hower and Uradnik[47] argue that the dependence on information technology makes countries vulnerable to cyberattacks and terrorism.

The *Tallinn Manual*,[48] which links his conception to Estonian events, addresses the issue of the international law applicable to cyberwarfare. The manual, prepared by the International Group of Experts at the Invitation of the CCDCOE and published in 2013, focuses on actions that qualify as self-defense and those taking place during armed conflict. Therefore, the first edition of the manual addresses topics including sovereignty, state responsibility, the *jus ad bellum*, international humanitarian law (IHL), and the law of neutrality. An extensive commentary accompanies each rule, which sets forth the rule's basis in treaty and customary law, explains how the group of experts interpreted applicable norms in the cyber context, and outlines any disagreements within the group as to each rule's application. The revised version of the manual released in 2017 focuses on the analysis of how existing international law applies to cyberspace.[49] The *Tallin Manual 2.0* expands its coverage of the international law governing cyber operations to peacetime legal regimes. The *Tallin Manual* reflects, on the one hand, the difficulty of legally framing the fight against cyberattacks and, on the other, the thin border between criminal attack and political act, whether it is conducted by and directed against states or by non-state organizations.

The United States, which is the main partner of NATO, has perceived the dangers of cyberthreats and has put in place a strategy to counter them. The Presidential Policy Directive 20 (PPD-20), signed by President Barack Obama in October 2012, provides a framework for US cybersecurity by establishing principles and processes.[50] The top-secret PPD-20 directive steps up offensive cyber capabilities to "advance US objectives around the world."

Executive Order 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* issued on May 11, 2017 by President Donald J. Trump (the cybersecurity EO), recognizes the urgency of cyber policy challenges and disposes to reinforce the integration between executive departments and federal agencies.[51] Pursuant to the cybersecurity EO, the US Department of State drafted two documents: *Recommendations to the*

President on Protecting American Cyber Interests through International Engagement[52] and *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*.[53]

In the above-mentioned documents published on May 31, 2018, the Department of State, acknowledging that cyberthreats must be addressed as both domestic and foreign policy priorities, calls to strengthen international cooperation in cyberspace, including cyber intelligence and military cyber cooperation. Both state actors and non-state actors, including criminals and terrorists, possess cyber capabilities that can be used to carry out malicious acts in peacetime, in periods of increasing international tensions, in crisis situations, and during armed conflicts.[54]

The State Department considers continued cyberattacks as use of force against the United States, its partners, and allies.[55] The choice among the wide variety of cyber and non-cyber options for deterring and responding to cyber activities that constitute a use of force lies in the hands of the president.[56] These options include the use of force provided by the *Authorization for Use of Military Force against Terrorists* (AUMF),[57] whose application has led to gross and continued violations of IHL sanctioned also by the US Supreme Court.

The cyberpolicy designed by the Office of the Coordinator for Cyber Issues includes the promotion of international commitments regarding what constitutes acceptable and unacceptable state behavior in cyberspace from all states and how international law applies to cyberspace. Therefore, the Department of State recognizes the need for an international legal framework on cyberdefense, whether the attacks come from state or non-state actors, especially regarding the use of force.

Cybersecurity is managed primarily by the Department of Homeland Security (DHS), through federal agencies such as the Federal Emergency Management Agency (FEMA); the US Department of Justice, through federal agencies such as the FBI; and the Central Intelligence Agency (CIA), part of the broader US Intelligence Community (IC), a federation of 16 separate agencies that work separately and together to conduct intelligence activities to support the foreign policy and national security of the nation. Member organizations of the IC include intelligence agencies, military intelligence, and civilian intelligence and analysis offices within federal executive departments. The IC is overseen by the Office of the Director of National Intelligence (ODNI), which itself is headed by the Director of National Intelligence (DNI), who reports to the president of the United States.

Cyberdefense and counter-cyberterrorism activities are carried out by the US armed forces. The purpose of the DoD cyberstrategy is to guide the development of DoD's cyber forces and strengthen the cyberdefense and cyber deterrence posture.[58] In July 2016 the US Cyber Command launched the Joint Task Force Ares (JTF-Ares), a unity of command and effort created

to coordinate cyberspace operations against the Islamic State with the Global Coalition against Daesh and with US Central Command (CENTCOM), which is leading the military fight and working to sharpen offensive operations against ISIS in Iraq and Syria.[59] Due to the expansion of the cyber operation of ISIS and other terrorist networks, the JTF-Ares is expected to go global in the future. In response to the changing face of warfare, in May 2018 the US Cyber Command (USCYBERCOM) was elevated to the 10th Department of Defense unified combatant command (COCOM).[60] In addition to USCYBERCOM, the DoD has a number of cyber centers: Army Cyber Command (ARCYBER); US Fleet Cyber Command (FCC)/US 10th Fleet (C10F); Air Forces Cyber (AFCYBER)/24th Air Force; US Marine Corps Forces Cyberspace Command (MARFORCYBER); US Coast Guard Office of Cyberspace Forces (CG-791); National Guard Cyber Units. The multiplication of cybercommands, one for each armed force, can be an overlapping and a waste of resources; it would be better to concentrate cyber capabilities in a single inter-force structure, regardless of the coordination exercised by the IC.

The US and NATO at War with Cyberterrorism

NATO and its allies, primarily the US, are defining a new defense doctrine on cyberwarfare. The Alliance acknowledges that "[t]hreats can come from state and non-state actors, including terrorism and other asymmetrical threats, cyberattacks and hybrid warfare, where the lines between conventional and unconventional forms of conflict become blurred."[61] At the NATO Summit held in Lisbon in November 2010, the North Atlantic Alliance claimed that terrorism poses a direct threat to security and international stability.[62] At the 2014 NATO Summit in Wales, allies recognized that international law applies in cyberspace, and that the impact of cyberattacks could be as harmful as a conventional attack. As a result, cyberdefense was recognized as part of NATO's core task of collective defense.[63] At the Warsaw Summit in 2016, allies took further action to recognize cyberspace as a domain of operations, just like air, land, and sea.[64] Cyberattacks are deemed to be a threat to national security and "vital interests" to be tackled with international partnership capacity in cybersecurity and cyberdefense.[65]

Article 5 of the North Atlantic Treaty, requiring partners to come to the aid of any member state subject to an armed attack, was invoked for the first and only time after the September 11 attacks at the request of the US, which gave rise to the intervention in Afghanistan.[66] Article 4, which merely invokes consultation among NATO members, has been invoked by Turkey in 2012 over the Syrian civil war, and in 2015 after threats by the Islamic State to the Turkish territorial integrity.[67] Both articles have been invoked in connection with hybrid conflicts,[68] which involve state and non-state

actors.[69] NATO is evolving in response to new strategic reality,[70] and terrorism is among the most pressing challenges the Alliance faces.

It is not just a question of resilience. While the US adapts to the challenges of cyberspace, this, by definition, requires international rules. So far, attempts to reach an agreement on which law to apply in cyberspace have failed. The US complains that the 2016–17 UN Group of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security failed to reach a consensus on cyberspace measures, including the *jus ad bellum*, IHL, and the law of state responsibility.[71] The right to make war (*jus ad bellum*) is recognized only for states, and the right to kill (*jus in bello*) is recognized only for the military.

When the GGEs examined for the first time the issue of information security in 2004/2005, the 15 members were not able to reach consensus on state exploitation of these activities for military and national security purposes.[72] The third GGEs (2012/2013) concludes that international law, in particular the UN Chart, applies to cyber-sphere, and that human rights and fundamental freedoms must be respected in addressing information security.[73] The group agrees that states must not use proxies to commit internationally unlawful acts and must ensure that their territories are not used by non-state actors to commit such acts.

Instruments on Cybercrime and Cyberterrorism

The first attempt to adopt a convention on terrorism was made in 1937 when, following the assassination of King Alexander of Yugoslavia and French Prime Minister Louis Barthou, the League of Nations (LN) prepared a draft *Convention for the Prevention and Punishment of Terrorism* and a draft plan for an International Criminal Court (neither of which ever entered into force). [74] Since 1963, the international society has elaborated many conventions for the prevention and suppression of international terrorism,[75] as well as a number of regional ones. So far, only a few regional anti-terrorism instruments consider cyberattacks to be acts of terrorism.

Article 1 of the *Treaty on Cooperation among the State Members of the Commonwealth of Independent States in Combating Terrorism* of 1999 includes cyberterrorism among acts of "technological terrorism." Section III (14) of the *Concept of Cooperation between Member States of the Shanghai Cooperation Organization in Combating Terrorism, Separatism, and Extremism* of 2005 adds cyberterrorism among the fundamental avenues of cooperation between member states. The Model Anti-Terrorism Law endorsed by the African Union (AU) in 2011 broadens the definition of terrorist act by including computer crimes. In 2007, the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) expressed the commitment to identify and fight cybercrime as

an emerging terrorist threat.[76] In 2016, the Organization of Islamic Conference (OIC) has considered adding an additional protocol on cyberspace terrorism to the *Convention on Combatting International Terrorism* of 1999.[77] So far, cyberterrorism is not mentioned in any Islamic CT convention, while jihadist terrorism remains the main transnational threat.

The Council of Europe (CoE) adopted two (inter-)regional instruments on cybercrime but failed to include cyberterrorism. Therefore, both the *Convention on Cybercrime* of 2001[78] and the Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of 2003[79] do not include cyberterrorism among proscribed acts.

The 2001 *Convention on Cybercrime* is the first international instrument on crimes committed via the Internet and other computer networks, dealing particularly with violations of network security. It has been ratified by 30 European countries and the US. The preamble of the Convention states that its main purpose is to establish a common criminal policy aimed at the protection of society against cybercrime. The 2013 EU Directive on attacks against information systems[80] does not go beyond the 2001 CoE Convention. Further regional instruments on cybercrime have been inspired by the latter.

Several regional, (inter-)regional, and subregional organizations have adopted instruments for combating cybercrime: the Models for Cyber Legislation in ESCWA Member Countries (EMCs) endorsed by the UN Economic and Social Commission for Western Asia in 2007; the League of Arab States *Convention on Combating Information Technology Offences* of 2010; the ECOWAS Directive on Fighting Cyber Crime of 2011; the Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Model Bill of 2011; the Electronic Crimes Bill developed by the Organization of Eastern Caribbean States (OECS) in 2011; the Model Law on computer crime and cybercrime adopted by the Southern African Development Community (SADC) in 2012; the Model Law on Cybercrime/e-Crimes, finalized in 2012 under the EU co-funded project HIPCAR (Harmonization of ICT Policies, Legislation, and Regulatory Procedures in the Caribbean); the Commonwealth Model Law on Computer and Computer-related Crime of 2014; and the *Convention on Cyber Security and Personal Data Protection* (AUCC) adopted by the AU in 2014.

In 2010, several UN member states called for an International Convention on Cybercrime.[81] The Commission on Crime Prevention and Criminal Justice (CCPCJ) reiterated the need to combat cybercrime.[82] In 2015, the thirteenth UN Congress on Crime Prevention and Criminal Justice debated whether or not a new cybercrime convention should be considered. The Congress addressed cybercrime jointly with terrorism, without making a distinction and without considering them as a *unicum*.[83] Although violence is necessary to characterize both crime acts and terrorist acts, it is not

sufficient to characterize the latter. The question arises of whether cybercrime is an autonomous and distinct offense from cyberterrorism. This raises the question of which means to employ and which laws apply to the war on cyberterrorism.

The War on Terror and International Law

Cyberattacks take place in cyberspace, which has become a virtual battlefield. Cyberdomain goes far beyond the boundaries of a traditional conflict. Therefore, the question arises whether international law, particularly IHL, apply to cyberwarfare against transnational non-state entities, such as terrorist groups and terrorist organizations.

As for international law, the sources of IHL are treaties and customary international law, which consists of rules that come from "a general practice accepted as law" and that exist independent of treaty law. Part of these norms are recognized as a fundamental principle of international law from which no derogation is permitted (*jus cogens*).

Among the treaties that constitute the IHL, an important role is played by the Geneva Conventions of 1949 and their Additional Protocols. The four Geneva Conventions are a set of rules that apply only in times of armed conflict (*jus in bello*) and that seek to protect people who are not or who are no longer taking part in hostilities. The whole set is referred to as the Geneva Conventions of 1949 or simply the Geneva Conventions.[84]

The 1949 Conventions have been modified with three amendment protocols: Protocol I (1977) relating to the *Protection of Victims of International Armed Conflicts*; Protocol II (1977) relating to the *Protection of Victims of Non-International Armed Conflicts*; and Protocol III (2005) relating to the *Adoption of an Additional Distinctive Emblem*.

The Geneva Conventions apply at times of war and armed conflict to governments who have ratified them. The Conventions apply to a signatory nation even if the opposing nation is not a signatory, but only if the opposing nation accepts and applies the provisions of the Conventions.[85] When the criteria of international conflict have been met, the full protections of the Geneva Conventions are considered to apply.

Common Article 3 relating to non-international armed conflicts states that the certain minimum rules of war apply to armed conflicts that are not of an international character but that are contained within the boundaries of a single country. This article refers to the territory of one of the High Contracting Parties. The applicability of this article rests on the interpretation of the term "armed conflict."[86] For example, it would apply to conflicts between the government and rebel forces, or between two rebel forces, or to other conflicts that have all the characteristics of war but that are carried out within the confines of a single country. A handful of individuals attacking a

police station would not be considered an armed conflict subject to this article, but subject only to the laws of the country in question.[87] The same should be said of criminals who commit a cyberattack.

It was said that Article 3 would cover in advance all forms of insurrection, rebellion, anarchy, and the break-up of states, and even plain brigandage and banditry, giving to a handful of rebels or common brigands the status of belligerents, and possibly even a certain degree of legal recognition.[88] There is also a risk that common or ordinary criminals give themselves an appearance of organization as an opportunity for requesting application of the Geneva Conventions, representing their crimes as "acts of war" in order to escape punishment for them.[89]

Sometimes insurgents are mere bandits, even if not all insurgents are bandits. Sometimes it happens in a civil war that the rebels are true patriots fighting for the independence of their country, and they should be considered genuine soldiers, not terrorists.[90] Ruling in favor of the Kurdish people and organizations alleged to support the Kurdistan Workers' Party (PKK), a left-wing organization labeled as terrorist by Turkey and Western governments, a Belgian criminal court underlined the fact that PKK undersigned the Protocols Additional to the Geneva Conventions and other international agreements and is not employing child soldiers.[91]

The other Geneva Conventions are not applicable in non-international armed conflicts, but only the provisions contained within Article 3, and additionally within the language of Protocol II. The rationale for the limitation is to avoid conflict with the rights of sovereign states that were not part of the treaties. When the provisions of this article apply, it states that persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed out of action (*hors de combat*) by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely.

For this purpose, Article 3(1) of Convention (IV) prohibits the following acts with respect to the people mentioned above: violence to life and person, in particular murder of all kinds, mutilation, cruel treatment, and torture; taking of hostages; outrages upon dignity, in particular humiliating and degrading treatment; and the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees that are recognized as indispensable by civilized peoples. Article 3(2) provides that the wounded and sick are collected and cared for.

Although at the time of the drafting of the Geneva Conventions it was thought that Common Article 3 could serve as a wildcard for all those situations of hybrid conflict, recent conflicts demonstrate that, as interpreted and applied, it is unsuitable to present challenges; cyberwarfare is more than a hybrid conflict—it is an asymmetrical threat.

Article 1(4) of the Additional Protocol I, by extending the scope of Article 3, includes the so-called wars of national liberation, deeming them to be international in nature. Article 1 of Additional Protocol II provides for its scope of application "dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory."[92] Additional Protocol II applies only to traditional interstate conflict, which requires control over territory by organized armed groups.[93] In the *Milošević* case, the International Criminal Tribunal for the former Yugoslavia (ICTY) ruled that control over territory by insurgents was not a requirement for the existence of a non-international armed conflict.[94] Carrying out cyberattacks does not require control of a territory, but only a computer.

The 1977 Protocols additional to the Geneva Conventions combine and update elements of the Hague law[95] and Geneva law, and they were issued in response to non-international armed conflicts and wars of national liberation that arose in the two decades following the adoption of the Geneva Conventions.

Along with the Geneva Conventions, the Hague Conventions were among the first formal statements of the laws of war and war crimes in the body of secular international law. The Geneva Conventions define the basic rights of wartime prisoners (civilians and military personnel), establish protections for the wounded and sick and for the civilians in and around a war zone, and define the rights and protections afforded to noncombatants. The Hague Conventions, adopted at the First Hague Conference of 1899[96] and at the Second Hague Conference of 1907,[97] regulate the use of weapons of war, along with the biochemical warfare Geneva Protocol.[98] Cyberweapons are not proscribed by the Hague Conventions; therefore, a cyberattack should be considered lawful.

Even if after 1977 the Geneva Conventions offer two separate regimes for non-international armed conflict—one covered by Common Article 3 with low threshold, and another falling within the scope of Additional Protocol II, whose threshold of application is high—in both cases it falls within the concept of armed conflict as defined, that is, not an incident or an occasional and low-intensity clash and involving military organizations.[99] The *Tadić* decision by the ICTY[100] is widely relied on as authoritative for the meaning of armed conflict in both international and non-international armed conflicts.[101]

The UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, wonders whether IHL applies in transnational armed conflict against non-state groups.[102] He asks whether there can exist a non-international armed conflict that has no finite territorial boundaries with a non-state armed group operating transnationally.[103] Emmerson wonders

when attacks caused by transnational, non-state organizations and by their affiliates satisfy the criteria to qualify as an armed conflict under IHL.[104]

The question arises whether a cyberattack committed by a transnational terrorist organization should be considered international or non-international conflict. Cyberwarfare, which takes place in cyberspace, is by definition an international conflict that goes far beyond any physical boundary. Article 3 applies only to conflicts of non-international character. The only alternative to Article 3 is Article 2, but this applies only to international conflicts between signatory states. Pretending to consider the cyberspace domain as a traditional domain and claiming to apply IHL for the sole purpose of lawfully using armed forces in contrast to cyberterrorism is a stretch.

Cyberprisoners of War

The law of war divides persons in the midst of an armed conflict into two broad categories: combatants and civilians.[105] This fundamental distinction determines the legal status of persons participating in or affected by combat and determines the legal protections afforded to such persons, as well as the legal consequences of their conduct. Combatants are those persons who are authorized by international law to fight in accordance with the law of war on behalf of a party to the conflict.[106] Civilians are not authorized to fight, but they are protected from deliberate targeting by combatants as long as they do not take up arms.[107] In order to protect civilians, the law of war requires combatants to conduct military operations in a manner designed to minimize civilian casualties and to limit the amount of damage and suffering to that which can be justified by military necessity.[108]

An enemy caught in the context of the war on cyberterrorism is not a virtual prisoner but a real one. If civilians participate in hostilities, they are not privileged under the law of war and may be prosecuted for it. At the same time, they do not incur the full liabilities attendant to "combatants status" (e.g., they do not enjoy the status of prisoners of war if captured) and can be targetable. Unless civilians adopt a continuous combat function, they cannot be targeted except for the periods they do participate in hostilities. And then there is the case of civilians participating in hostilities without taking up arms, but with a supporting role. Therefore, how to treat civilians carrying out cyberattacks? We are not talking about non-regular fighters carrying arms, but about civilians engaged in cyberwarfare.

Walzer[109] and Fletcher[110] agree that irregulars in civilian clothes do not meet the rules of war and hence are not eligible for protection. In analyzing guerrilla warfare, Walzer infers that insurgents, dressed in civilian clothes, morally defy the most fundamental rules of war by not wearing a uniform that distinguishes them from regular soldiers.[111] Saul suggests that a narrow

class of terrorist acts may be excused by individual or group defenses and considered to be "collective defense of human rights."[112] Cullen concludes that, before World War II, three types of actors were identifiable in non-international conflicts[113]: rebels, insurgents, and belligerents. The last two are both armed fighters, but only belligerents have a privileged combatant status under IHL.[114]

The question is if the provisions of the Geneva Conventions apply to all combatants. Gill and van Sliedregt argue that the war on terror, "whatever else it is…is not a international armed conflict in a legal sense."[115] The Dutch scholars acknowledge that the military operations against the Taliban and al-Qaeda in Afghanistan do qualify as international armed conflict to which the laws and customs of war, including the notion of combatant status, must be applied.[116]

The Bush administration had contended that the laws and customs of war did not apply to the US armed conflict with al-Qaeda fighters during the 2001 US invasion of Taliban-controlled Afghanistan. In *Hamdan v. Rumsfeld*[117] the US Supreme Court (SCOTUS) ruled that Common Article 3 does apply in such a situation, which requires fair trials for prisoners.[118] The SCOTUS stated that the Third Geneva Convention and Article 3 of the Fourth Geneva Convention (requiring humane treatment) apply to all detainees in the WoT. Common Article 3 applies in "wars not of an international character" (i.e., civil wars), in a signatory to the Geneva Conventions, and the civil war was in signatory Afghanistan.

Meisels thinks that selective application of the rules of war is not a morally viable option, and that none of the parties can demand their protection without assuming their burdens.[119] Statman writes that conventions require mutuality, and that groups such as al-Qaeda and Hamas do not abide by them.[120] In the commentary published in 1952, the director for General Affairs of the International Committee of the Red Cross, Jean S. Pictet, argues that it would be impossible to constrain provisional governments, or political parties, or groups not yet in existence, by a convention.[121] Nevertheless, as we have seen, not all proscribed organizations, e.g., the PKK, avoid applying the laws of war. Contrariwise, it might be inferred that if a "terrorist" group abides by the conventions, these are to be applied to it. In fact, if we assume as true the claim that if one side violates a convention, the other side is released from its contractual commitment to respect it,[122] then we should deduce that it is legal for one party to breach a convention following the same violation by the counterpart. For example, if a Western government, such as the United States, violates a convention, it is legitimate for its opponents acting accordingly.

Article 51 of Protocol I requires states to comply anyway with their obligation to respect civilians, even if these obligations are breached by the counterpart.[123] Someone could say that conventional laws of war are

updated,[124] and this is probably true, but if they are not fulfilled, the boundary between what is permissible and what is illicit would be entrusted exclusively to moral evaluations.

In the Commentary to Geneva Convention (IV), Pictet,[125] regarding Article 4, writes:

Every person in enemy hands must have some status under international law: he is either a prisoner of war and, as such, covered by the Third Convention, a civilian covered by the Fourth Convention, [or] a member of the medical personnel of the armed forces who is covered by the First Convention. *There is no* intermediate status; nobody in enemy hands can fall outside the law.

Thus if detainees are not considered prisoners of war, this would still grant them the rights of the Fourth Geneva Convention, as opposed to the more common Third Geneva Convention, which deals exclusively with prisoners of war (POWs).

After the establishment of the Guantánamo Bay detention camp in January 2002, with the purpose to detain extraordinarily dangerous people, to interrogate detainees in an optimal setting, and to prosecute detainees for war crimes,[126] in February 2002 the White House determined that Taliban detainees were covered under the Geneva Conventions, while al-Qaeda terrorists were not, but that none of the detainees qualified for the POW status under Article 4 of the Third Geneva Convention.[127] The US administration deemed all of the detainees, including individuals who never were close to a battlefield and who were captured thousands of miles from a battle zone, to be "unlawful enemy combatants" who may be held indefinitely without trial, depending on how long America's war on terrorism lasts.[128] These include nationals of countries that are not at war with the United States.[129]

It is not clear on which basis al-Qaeda is a belligerent under the law of war, because it does not qualify and because such a status would imply rights that the US administration has been unwilling to concede. Another question is how the United States can apply Article 3, which applies to non-international conflicts, to "not POWs" who are citizens of a country, Afghanistan, which is not at war with Washington. This is a contradiction frequently emphasized in the rulings delivered by US courts.

The US administration argued that the non-application of POW status to the Taliban is because they do not effectively distinguish themselves from the civilian population—they do not wear uniforms and insignia, and they do not carry weapons outside—and do not conduct their operations in accordance with the laws and customs of war.[130] According to the Hague Convention IV of 1907, in order to be entitled to POW status, fighters must wear "a fixed distinctive sign visible at a distance" and must "carry their arms openly."[131] Can you imagine a cyberterrorist carrying his laptop "openly"?

Even if President George W. Bush determined that the Afghan Taliban were not entitled to POW status under Geneva Convention (III), the Taliban fighters associated with both the Taliban and al-Qaeda are protected under the Convention on the basis that Afghanistan was a High Contracting Party to the Convention,[132] although then Kabul government (1996–2001) was not recognized by the US.[133] The District Court for the District of Columbia ruled that the Third Geneva Convention does not permit the determination of POW status in such a political way, as the Convention is self-executive.[134]

Article 5 of Geneva Convention (III) entitles individuals detained under Article 4, including members of militias or volunteer corps and members of organized resistance movements, to be treated as POWs until a "competent tribunal" determine their status. In accordance with that provision in 2004 the US administration established the Combatant Status Review Tribunals (CSRTs), a set of tribunals coordinated through the Office for the Administrative Review of the Detention of Enemy Combatants.[135]

In *Hamdan v. Rumsfeld* the Supreme Court holds that President Bush did not have authority to set up the war crimes tribunals and finds the special military commissions illegal under both military justice law and the Geneva Conventions. Hamdan was not a member of the US military and would be tried before a military "commission," not a court-martial, which does not meet the requirements of Article 21 of the Uniform Code of Military Justice (UCMJ) or of Article 102 or the Geneva Convention (III), and therefore violates the laws of war. Hence, the SCOTUS finds that CSRTs do not qualify as "competent tribunals" under the provision of Article 5 of the Third Geneva Convention.

Here arises the question whether insurgents could be legally bound by a convention that they had not themselves signed.[136] According to Pictet, if an insurgent party does not apply Article 3, it will prove that those who regard its actions as mere acts of anarchy or banditry are right.[137]

In the light of the intervention of foreign powers, it is hard to claim that the Syrian conflict, as well as the Afghan insurgency, is a civil war. Involvement of many national forces in military operations characterize these conflicts as international conflicts. If the war on (cyber)terrorism is a global conflict against non-state actors, governments should comply with IHL.

De jure governments are afraid to increase the authority of rebels by constituting an implicit recognition of the legal existence and belligerent status of the party concerned through application of Article 3.[138] For this purpose, Article 3(4) makes absolutely clear that the object of the Geneva Conventions is purely humanitarian, lacking of effect on the legal status of the parties to the conflict; it does not confer belligerent status and, consequently, increased authority onto the adverse party.[139]

Governments are obliged to apply all the provisions embedded in domestic and international human law. Failure to apply these provisions should be considered a grave breach. Klabbers claims that there is no good reason for refusing to terrorists the protection granted by IHL[140]; they have the right to be treated humanely, even if the law does not provide for it in a clear manner.[141]

Article 17 of the 1998 *International Convention for the Suppression of Terrorist Bombings* provides the application of international law, including IHL, to terrorists.[142] Under Article 19(2) of the Convention, however, the activities of armed forces during an armed conflict, and the activities undertaken by military forces of a state in the exercise of their official duties, are not governed by IHL. The notion of "armed forces" appears to include non-state armed groups that are party to an armed conflict. Klabbers concludes that the issue of whether IHL applies to terrorism is due to political ambivalence.[143]

Lieber believes that captured belligerents must be treated as prisoners of war.[144] Ipsen thinks that the fundamental distinction between lawful and unlawful combatants is between persons who are entitled to POWs status and those who are not.[145] Thus captured enemies would fail to qualify as POWs because they fail to meet the legal qualification of lawful belligerent.

Meisels argues that irregular combatants are legitimately considered unlawful, and thus duly denied the rights of regular soldiers, but, once captured and disarmed, they must enjoy some minimal standard of international humanitarian treatment.[146] She assumes that the distinction between lawful and unlawful combatants lies in the difference between combatants and civilians.[147]

Nabulsi thinks that, as in the traditional laws of war only professional soldiers are granted belligerent status, all civilians are considered outlaws.[148] She gathers that the law of war drafted in the Hague and in the Geneva Conventions serves the powerful and the strong.[149] Nabulsi refuses the inflexible distinctions drawn by laws of war between civilians and combatants and the offshoot distinction between lawful and unlawful combatants.[150] According to the American-born scholar, the distinction of combatants from civilians, and the derivative difference between lawful and unlawful combatants, are set up in an international legal system to favor states over irregulars.[151] Nabulsi concludes that the distinction between the former and the latter was never resolved in international law,[152] and hence the term "unlawful combatant" has become controversial, and now problematic.[153]

If irregular combatants are not protected under the Geneva Convention (III), as they are not considered members of regular armed forces, then they should be considered civilians and then protected according to Geneva Convention (IV) and Additional Protocols I and II. It is left open the question of when "unlawful enemy combatants" have to be considered

terrorists, and when they rather have to be considered insurgents, rebels, or irregular opponents, whatever one calls them.

As you can see, applying to terrorism and cyberterrorism, in particular, international law and IHL, hides many pitfalls. One of these pitfalls, the last we analyze in this article, is represented by the nature of cyberattacks.

(Cyber)War Is Not an Armed Conflict

Considering that in the fight against terrorism there is no clearly identifiable enemy, the war on cyberterrorism seems to be a worldwide operation against hostile governments and hostile nation-state actors (terrorist groups, criminal organizations), rather than a classical defensive or aggressive war against a country or a coalition of states.

The European Commission for Democracy through Law (the Venice Commission) established by the Council of Europe finds that "sporadic bombings and other violent acts which terrorist networks perpetrate in different places around the globe and the ensuing counter-terrorism measures, even if they are occasionally undertaken by military units, cannot be said to amount to an 'armed conflict' in the sense that they trigger the applicability of International Humanitarian Law."[154] The Venice Commission holds that "organized hostilities in Afghanistan before and after 2001 have been an 'armed conflict' which was at first a non-international armed conflict, and later became an international armed conflict after the involvement of US troops"[155]—a real war, thus in violation of international law. The Venice Commission considers that CT measures that are part of the war on terror are not part of an armed conflict in the sense of making the regime of IHL applicable to them.[156] IHL is an instrument to define a conflict, and vice versa.

Sir Christopher Greenwood, an English judge at the International Court of Justice (ICJ), observes that "many isolated incidents, such as border clashes and naval incidents, are not treated as armed conflicts."[157] Sir Greenwood infers that "only when fighting reaches a level of intensity which exceeds that of such isolated clashes will it be treated as an armed conflict to which the rules of international humanitarian law apply."[158]

The Use of Force Committee established by the International Law Association (ILA) finds that the term "war," while still used, has, in general, been replaced in international law by the broader concept of armed conflict,[159] which, lacking a multilateral treaty that provides a generally applicable definition, remains unclear and subject to customary international law and subsidiary sources. For governments is open the road to free will.

In international law the term "war" seems to have no longer the same significance it used to have: "a contention between two or more [s]tates through their armed forces, for the purpose of overpowering each other

and imposing such conditions of peace as the victor pleases."[160] The Use of Force Committee report concludes that "the concept of armed conflict has largely replaced the concept of war" and that "earlier practice of states creating a *de jure* state of war by a declaration is no longer recognized in international law."[161] This practice has significant wide-ranging implications for the discipline of international law such as treaty obligations.[162]

The ILA Committee considers that defining an armed conflict as fighting between organized armed groups renders the concept applicable both to sovereign states and non-state actors engaged in fighting of some intensity, not just in declared wars.[163] This is not a situation where governments simply declare their policy preferences.[164]

The *Final Report on the Meaning of Armed Conflict in International Law* was motivated by the United States' position following the 9/11 attacks, claiming the right to exercise belligerent privileges applicable only during armed conflict anywhere in the world where members of terrorist groups are found. The US position was contrary to a trend by states attempting to avoid acknowledging involvement in wars or armed conflicts.[165]

The report led to the conclusion that the provisions of the Geneva Conventions apply to any conflict, even if it is not declared or formally termed as a war. Thus armed groups, including Islamic organizations, are to be considered combatants to all effects, and the IHL should apply to them. The US government, by creating a new military, political, and legal language, in order to support the use of tools and typical methods of conventional warfare in unconventional conflicts, finds itself in a state of unlawfulness.

Common Article 3, which applies in non-international armed conflicts, provides criteria to distinguish it from lesser forms of violence.[166] The intensity of the conflict[167] and the organization of the parties are the sole criteria to distinguish an armed conflict from "banditry, unorganized and short-lived insurrections, or terrorist activities."[168] These criteria seem to be widely accepted in international jurisprudence (see the International Criminal Tribunal for Rwanda[169] and the International Criminal Tribunal for the former Yugoslavia).[170] An exception is the *Mucić* case, in which the ICTY ruled that "the existence of armed force between states is sufficient of itself."[171]

In a cyber conflict there would be no casualties, nor would it be possible to ascertain any war crimes or crimes against humanity. And, to make a paradox, how to consider young hackers, when recruitment of children is prohibited under international law?[172] All these issues demonstrate the inadequacy of the current rules and the inability to apply them to asymmetrical threats and hybrid conflicts.

Conclusions and Recommendations

In this article, we have assessed whether human rights law and the law of war, which are a branch of international law, apply to the war on cyberterrorism.

The threat to security is not enough to characterize an action as an act of terrorism. If we compare cyberterrorism to cyberwarfare, or to a form of conventional conflict, it should be noted that cyberterrorism or cyberwarfare cannot be considered a conventional conflict, a war, although the component of violence is present in both cyberevents. Even considering cyberwarfare as a traditional armed conflict, we must keep in mind that a war should have a temporal, physical space: a territory where the clash occurs and beginning and end of hostilities. The termination of hostilities is essential for the release of prisoners of war. This is another weak point in support of cyberwarfare's equalization of a conventional conflict, as well as the need to define the theater of operations, which in cyberspace is virtual and unlimited.

Another critical issue is the difference between cyberattacks carried out by non-state entities, such as rebel groups or terrorist organizations, and those sponsored by governments. Therefore, I believe that non-state cyberterrorism should be treated as a form of ordinary crime, applying the tools already available, while state-sponsored cyberattacks can apply the NATO doctrine, which equates the cyber domain with the three traditional domains. This doctrine needs to meet international humanitarian law and the law of war.

Before identifying the means and strategies to tackle it, we recommend that the international community defines what cyberterrorism is. This presupposes, upstream, the "impossible mission" to define the mother term "terrorism." A definition should be precise and narrow to permit the legitimate prosecution of criminal acts. A legal rule is needed to assess whether a behavior is lawful or not. IHL can be adapted, in some way, to cyberwarfare through customary law, but meeting the limit of *jus cogens*.

ORCID

Marco Marsili http://orcid.org/0000-0003-1848-9775

Notes

1. Carlos Fernando Diaz-Paniagua, "Negotiating Terrorism: The Negotiation Dynamics of Four UN Counter-terrorism Treaties, 1997–2005" (PhD dissertation, City University of New York, 2008), 47.
2. Alex P. Schmid (ed.), *The Routledge Handbook of Terrorism Research* (London: Taylor & Francis, 2009), 39. See also Myra Williamson, *Terrorism, War and International*

Law: The Legality of the Use of Force against Afghanistan in 2001 (Farnham: Ashgate, 2008), 38.
3. Ben Saul, *Defining Terrorism in International Law* (Oxford: Oxford University Press, 2006), 11.
4. Sami Zeidan, "Desperately Seeking Definition: The International Community's Quest for Identifying the Specter of Terrorism," *Cornell International Law Journal* 36 (2004): 491–92.
5. Barry Collin, "The Future of Cyberterrorism," *Crime & Justice International Journal*, Vol. 13, no. 2 (March 1997): 15.
6. US Department of Defense, "The Department of Defense Cyberstrategy," https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed July 12, 2017).
7. Morrie Gasser, *Building a Secure Computer System* (New York: Van Nostrand Reinhold, 1988), 3.
8. Paul Everard, "NATO and Cyber Terrorism," in *Responses to Cyber Terrorism*, ed. Centre of Excellence Defence against Terrorism, Ankara, Turkey, NATO Science for Peace and Security Series, E: Human and Societal Dynamics, vol. 34 (Washington, DC: IOS Press, 2008), 119.
9. Jonathan Matusitz, "Cyberterrorism," *American Foreign Policy Interests* 2 (2005): 137–47.
10. Daphna Canetti, Michael Gross, Israel Waismel-Manor, Asaf Levanon, and Hagit Cohen, "How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks," *Cyberpsychology, Behavior, and Social Networking* 20, no. 2 (2017): 72–77.
11. Sara Hower and Kathleen Uradnik, *Cyberterrorism*, 1st ed. (Santa Barbara, CA: Greenwood, 2011), 140–49.
12. Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law* 43, no. 1 (2010).
13. Michael Erbschloe, *Information Warfare: How to Survive Cyber Attacks* (New York: Osborne/McGraw-Hill, 2001).
14. Maura Conway, "What Is Cyberterrorism?," *Current History* 101, no. 659 (2002): 436–42.
15. Jan Klabbers, "Rebel with a Cause? Terrorists and Humanitarian Law," *European Journal of International Law* 14, no. 2 (2003): 299–312, 310, https://doi.org/10.1093/ejil/14.2.299.
16. Ed Morgan, "International Law's Literature of Terror," *Canadian Journal of Law & Jurisprudence* 15 (2002): 217–324, 324, https://doi.org/10.1017/S0841820900003647.
17. Ali Khan, "A Legal Theory of International Terrorism," *Connecticut Law Review* 19, no. 945 (1987): 495.
18. Bruce Hoffman, *Inside Terrorism*, 2nd ed. (New York: Columbia University Press, 2006), 41.
19. Alex P. Schmid, "Terrorism: The Definitional Problem," *Case Western Reserve Journal of International Law* 36, no. 2 (2004): 375–419, 391.
20. Jan Klabbers, *Rebel with a Cause? Terrorists and Humanitarian Law*, 301.
21. Jean S. Pictet, *Geneva Conventions of 12 August 1949: Commentary. Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (Geneva: International Committee of the Red Cross, 1952), 39.
22. Ibid., 50, 52.

23. Tamar Meisels, "Combatants—Lawful and Unlawful," *Law and Philosophy* 26, no. 1 (2007): 31–65, 33, https://doi.org/10.1007/s10982-005-5917-2.
24. Ibid., 51.
25. Ibid.
26. Chrisje Brants, "Dealing with the Holocaust and Collaboration: The Dutch Experience of Criminal Justice and Accountability after World War II," *Crime, Law, & Social Change* 34, no. 3 (2000): 211–36, 211, https://doi.org/10.1023/A:1008358428102.
27. Ministry of Culture and Information of Saudi Arabia (ed.), *The Kingdom versus Terrorism: Stances and Achievements*, 1st ed. (Riyadh: Al-Quiman Multimedia, 2010), 20.
28. Mahmoud Cherif Bassiouni, "Terrorism: The Persistent Dilemma of Legitimacy," *Case Western Reserve Journal of International Law* 36, nos. 2–3 (2004): 299–306, 305.
29. Rosalyn Higgins, "The General International Law of Terrorism," in *International Law and Terrorism*, edited by Rosalyn Higgins and Maurice Flory (London: Routledge, 1997), 28.
30. Ibid.
31. Jan Klabbers, *Rebel with a Cause? Terrorists and Humanitarian Law*, 308.
32. Ben Saul, "Reasons for Defining and Criminalizing 'Terrorism' in International Law" (October 29, 2008), *Mexican Yearbook of International Law* 6 (2006): 419–60; Sydney Law School Research Paper no. 08/121, 220–21, https://ssrn.com/abstract=1291567.
33. Gregory D. Grove, "Cyber-attacks and International Law," *Survival* 42, no. 3 (2000): 89–103.
34. Lorenzo Valeri and Michael Knights, "Affecting Trust: Terrorism, Internet, and Offensive Information Warfare," *Terrorism and Political Violence* 12, no. 1 (2000): 15–36.
35. Timothy Shimeall, "Countering Cyber War," *NATO Review* 49 (2001): 16–18.
36. Jonalan Brickey, "Capturing a Broad Range of Activities in Cyberspace," *CTC Sentinel* 5, no. 8 (2012): 4–6.
37. Christopher Heffelfinger, "The Risks Posed by Jihadist Hackers," *CTC Sentinel* 6, no. 7 (2013): 1–5.
38. John Arquilla and David Ronfeldt (eds.), *Networks and Netwars* (Santa Monica, CA: Rand Corporation, 2001), 5–7.
39. Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (New York: Columbia University Press, 2015).
40. Gary R. Blunt, *Islam in the Digital Age: E-Jihad, Online Fatwas, and Cyber Islamic Environments* (London: Pluto Press, 2003), 47.
41. Ibid., 52–53.
42. Imran Awan and Brian Blakemore, *Policing Cyber Hate, Cyber Threats, and Cyber Terrorism* (Farnham: Ashgate, 2012).
43. Thomas J. Holt, George W. Burruss, and Adam M. Bossler, *Policing Cybercrime and Cyberterrorism* (Durham, NC: Carolina Academic Press, 2015).
44. Lee Jarvis, Stuart MacDoland, and Thomas M. Chen (eds.), *Terrorism Online: Politics, Law, and Technology* (London: Routledge, 2016).
45. Ibid., 166.
46. CCDCOE, "About Us," https://ccdcoe.org/about-us.html (accessed May 30, 2018).
47. Sara Hower and Kathleen Uradnik, *Cyberterrorism*, 140–49.
48. Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).
49. Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2017).

50. Barack Obama, *Presidential Policy Directive 20* (Washington, DC: The White House, 2012).
51. E.O. 13800 § 1(b)(iv).
52. Office of the Coordinator for Cyber Issues, *Recommendations to the President on Protecting American Cyber Interests through International Engagement* (Washington, DC: US State Department, 2018).
53. Office of the Coordinator for Cyber Issues "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats" (Washington, DC: US State Department, 2018).
54. Ibid.
55. Ibid.
56. Ibid.
57. *Authorization for Use of Military Force* (AUMF), Pub. L. 107–40, 115 Stat. 224 (50 U. S.C. § 1541).
58. US Department of Defense, *The DoD Cyber Strategy* (Washington, DC: DoD, 2025).
59. Cheryl Pellerin, "Cybercom: Pace of Cyberattacks Have Consequences for Military, Nation," https://www.defense.gov/News/Article/Article/1192583/cybercom-pace-of-cyberattacks-have-consequences-for-military-nation (accessed April 22, 2018).
60. US Cyber Command, "US Cyber Command History," http://www.cybercom.mil/About/History (accessed May 22, 2018).
61. NATO, "Resilience and Article 3," http://www.nato.int/cps/en/natohq/topics_132722.htm?selectedLocale=en (accessed June 30, 2016).
62. NATO, "Countering Terrorism," http://www.nato.int/cps/en/natohq/topics_77646.htm (accessed June 30, 2016).
63. NATO, "NATO Cyber Defence Fact Sheet," http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/20170515_1705-factsheet-cyber-defence-en.pdf (accessed May 25, 2017)
64. Ibid.
65. US Department of Defense, *The Department of Defense Cyberstrategy* (Washington, DC: DoD, 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed July 12, 2017).
66. NATO, "Invocation of Article 5 Confirmed," http://www.nato.int/docu/update/2001/1001/e1002a.htm (accessed June 30, 2016).
67. NATO, "The Consultation Process and Article 4," http://www.nato.int/cps/en/natolive/topics_49187.htm (accessed June 30, 2016).
68. For a definition of the term "hybrid conflict," see Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005).
69. Paul Gilbert, *New Terror, New Wars* (Edinburgh: Edinburgh University Press, 2003), 7–8.
70. Cheryl Pellerin, "Mattis: NATO Is Evolving in Response to New Strategic Reality," DoD News, Defense Media Activity, February 16, 2017, https://www.defense.gov/News/Article/Article/1085796/mattis-nato-is-evolving-in-response-to-new-strategic-reality (accessed February 17, 2017).
71. Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm (accessed June 27, 2017).
72. Report of the Secretary-general, "Developments in the Field of Information and Telecommunications in the Context of International Security" (UN Doc. A/60/202, UN, New York, NY, 2005). See also United Nations Office for Disarmament Affairs

(UNODA) "Fact Sheet July 2015," https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/04/Information-Security-Fact-Sheet-Apr2017.pdf (accessed June 27, 2017).

73. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (Report A/68/98, UN, New York, NY, 2013).
74. *Convention for the Prevention and Punishment of Terrorism*, done at Geneva on November 16, 1937, *League of the Nations Official Journal*, January 1938, Serie 1937, vol. 10, no. C.546.M.383.1937.V, p. 22.
75. UN Web Services Section, Department of Public Information, "United Nations Action to Counter Terrorism," http://www.un.org/en/terrorism (accessed April 11, 2016).
76. *Declaration of Panama on the Protection of Critical Infrastructure in the Hemisphere in the Face of Terrorism*, adopted at the CICTE Third Plenary Session held at Panama City on March 1, 2007, CICTE/DEC. 1/07, OEA/Ser.L/X.2.7.
77. OIC, "OIC to Revisit Convention on Combating International Terrorism," http://www.oic-oci.org//topic/?t_id=11148&t_ref=4385&lan=en (accessed May 13 2017).
78. *Convention on Cybercrime*, done at Budapest on November 23, 2001, ETS No. 185.
79. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, done at Strasbourg on January 28, 2003, ETS No. 189.
80. *Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*.
81. UN General Assembly Resolution 65/230 (A/RES/65/230) of December 21, 2010, adopted on the recommendation of the Economic and Social Council.
82. CCPCJ Res. 22/8. See also CCPCJ Res. 22/7, UNODC/CCPCJ/EG.4/2011/3 and UNODC/CCPCJ/EG.4/2013/3.
83. UN, "UN Congress Plenary Debate Focuses on Innovative Tools to Fight Cybercrime, Terrorism Recruitment, Wildlife Trafficking, among New, Emerging Threats," https://www.un.org/press/en/2015/soccp365.doc.htm (accessed June 10, 2017).
84. Final Act of the Diplomatic Conference of Geneva 1949, in UNTS vol. 75, nos. 970–973 (1950), 5 et seq.
85. Art. 2 of the Geneva Convention (I) of 1949.
86. Jean S. Pictet, *Geneva Conventions of 12 August 1949: Commentary. Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 49.
87. Ibid.
88. Ibid., 43, 44, 49.
89. Ibid., 44.
90. Ibid.
91. *The Public Prosecutor v. The Turkish State & Others*, Decision of November 3, 2016, the Dutch language court of first instance of Brussel - 41st Chamber (Penal Council Chamber), Investigation Office no. 2009/0030 - 2008/0113 - 2008/0121, Federal Prosecutor application no. FD.35.98.54/09 - FD.35.98.634/06-FD.35.98.502/07), 11.
92. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, done at Geneva on June 8, 1977.
93. Use of Force Committee, "Final Report on the Meaning of Armed Conflict in International Law" (The Hague Conference, International Law Association, May 2010), 12.

94. *Prosecutor v. Milosević*, Case No. IT-02-54-T, Decision on Motion for Judgement of Acquittal of June 16, 2004, para. 36.
95. *Convention (IV) respecting the Laws and Customs of War on Land and Its annex: Regulations concerning the Laws and Customs of War on Land*, done at The Hague on October 18, 1907.
96. *Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land*, done at The Hague on July 29, 1899.
97. *Convention (IV) respecting the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land*, done at The Hague on October 18, 1907.
98. *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare*, done at Geneva on June 27, 1925.
99. Use of Force Committee, *Final Report on the Meaning of Armed Conflict in International Law*, p. 13.
100. *Prosecutor v. Tadić*, Case No. IT-94-1-T, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction of October 2, 1995, para. 70.
101. *Prosecutor v. Akayesu*, Case No. ICTR-96-4-T, judgment of September 2, 1998, paras. 619–27.
102. Ben Emmerson, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" (A/HRC/25/59, GE.14-11949, UN, New York, NY, 2014), para. 71(g). See also the Special Rapporteur's interim report to the General Assembly, A/68/389, paras. 70–72; and the report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, A/68/382, paras. 69–71.
103. Ibid., para. 71(c). See also A/68/389, paras. 62–65; A/68/382, paras. 64–66.
104. Ibid., para. 71(e). See also A/68/389, paras. 66–69; A/68/382, paras. 55–63. For a comprehensive and up-to-date assessment of the threat of armed attack by al-Qaeda and its various affiliate organizations, and the degree of operational coordination, organization, and leadership among the various groups, see the fifteenth report of the Analytical Support and Sanctions Monitoring Team established pursuant to SC Resolution 1526 (2004), transmitted with the letter dated 22 January 2014 from the Chair of the Security Council Committee pursuant to Resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaeda and associated individuals and entities addressed to the President of the Security Council (S/2014/41).
105. Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflicts* (New York: Oxford University Press, 1995), 65.
106. Ibid., 67. See also Hilaire McCoubrey, *International Humanitarian Law: Modern Developments in the Limitation of Warfare*, 2nd ed. (Dartmouth, NH: Ashgate, 1998), 133–34.
107. Ingrid Detter, *The Law of War*, 2nd ed. (New York: Cambridge University Press, 2000), 285–88.
108. Jean S. Pictet, *Humanitarian Law and the Protection of War Victims* (Geneva: Henry Dunant Institute, 1975), 31.
109. Michael Walzer, *Just and Unjust Wars* (New York: Basic Books, 1977), 179–83.
110. George P. Fletcher, *Romantics at War: Glory and Guilt in the Age of Terrorism* (Princeton, NJ: Princeton University Press, 2003), 108.
111. Tamar Meisels, *Combatants—Lawful and Unlawful*, 45–46.
112. Ben Saul, *Defining Terrorism in International Law*, 69.

113. Anthony Cullen, *The Concept of Non-International Armed Conflict in International Humanitarian Law* (Cambridge: Cambridge University Press, 2010), 7–23.
114. Ibid.
115. Terry Gill and Elies van Sliedregt, "Guantánamo Bay: A Reflection on the Legal Status and Rights of 'Unlawful Enemy Combatants,'" *Utrecht Law Review* 1, no. 1 (2005): 28.54, 30–31, http://doi.org/10.18352/ulr.2.
116. Ibid.
117. *Hamdan v. Rumsfeld et al.* (05–184), 548 U.S. 557 (2006), decided on June 29, 2006.
118. Art. 3, para. 1(c) reads: "the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples."
119. Tamar Meisels, *Combatants—Lawful and Unlawful*, 50.
120. Daniel Statman, "Targeted Killing" *Theoretical Inquiries in Law* 5, no. 1 (2004): 179–98, 195.
121. Jean S. Pictet, *Geneva Conventions of 12 August 1949: Commentary. Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 42.
122. Jeff McMahan, "The Ethics of Killing in War," *Philosophia*, 34, no. 1 (2006), 25, 46–47, 10.1007/s11406-006-9007-y. Originally appeared in *Ethics* 114 (2004): 693–733.
123. *Protocol (I) additional to the Geneva Conventions of August 12, 1949, and relating to the protection of victims of international armed conflicts*, adopted on June 8, 1977, Art. 51(8).
124. Jeff McMahan, *The Ethics of Killing in War*, 39.
125. Jean S. Pictet (ed.), *Commentary on the Fourth Geneva Convention* (Geneva: International Committee of the Red Cross, 1958), 51.
126. US Department of Defense, "DoD News Briefing: Secretary Rumsfeld and Gen. Pace," http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=2254 (accessed July 4, 2016).
127. Lawrence Ari Fleischer, "White House Press Secretary Announcement of President Bush's Determination re Legal Status of Taliban and Al Qaeda Detainees," http://www.state.gov/s/l/38727.htm (accessed July 8, 2016).
128. *In re Guantánamo Detainees Cases*, Civil Action No. 02–299, decided on January 31, 2005, Memorandum Opinion by Judge Joyce Hens Green, in *Federal Supplement*, vol. 335, 2nd Series, 443.
129. *Rasul et al. v. Bush et al.* (03–334), 542 U.S. 466, 124 S. Ct. 2686, decided on June 28, 2004.
130. Lawrence Ari Fleischer, *White House Press Secretary announcement of President Bush's determination re legal status of Taliban and Al Qaeda detainees.*
131. *The Hague Convention (IV) of 1907 respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*, § I, ch. I, Art. 1; *Geneva Convention relative to the Treatment of Prisoners of War of August 12, 1949*, Part I, Art. 4.
132. *In re Guantánamo Detainees Cases.*
133. Adrian Guelke, *Terrorism and Global Disorder* (London: I.B. Tauris, 2006), 55.
134. *In re Guantánamo Detainees Cases.*
135. US Department of Defense, *Combatant Status Review Tribunals*, CSRT Info 26Sep06, v3F (Washington, DC: US DoD, 2006), http://archive.defense.gov/news/Oct2006/d20061017CSRT.pdf (accessed January 28, 2016).
136. Jean S. Pictet, *Geneva Conventions of 12 August 1949: Commentary. Volume I: For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the* Field, 52.

137. Ibid.
138. Ibid., 60.
139. Ibid., 61.
140. Jan Klabbers, *Rebel with a Cause? Terrorists and Humanitarian Law*, 311.
141. Ibid., 299.
142. *International Convention for the Suppression of Terrorist Bombings*, adopted by resolution A/RES/52/164 of the UN General Assembly on December 15, 1997, 2149 UNTS 284; 37 ILM 249 (1998); [2002] ATS 17.
143. Jan Klabbers, *Rebel with a Cause? Terrorists and Humanitarian Law*, 301.
144. Francis Lieber, *Guerrilla Parties Considered with Reference to the Laws and Usages of War* (New York: D. Van Nostrand, 1862).
145. Knut Ipsen, "Combatants and Non-Combatants," in *The Handbook of Humanitarian Law in Armed Conflicts*, ed. Dieter Fleck, (New York, Oxford University Press, 1995), 65–66. See also Article 4 of the Third Geneva Convention.
146. Tamar Meisels, *Combatants—Lawful and Unlawful*, 34.
147. Ibid., 64
148. Karma Nabulsi, *Traditions of War: Occupation, Resistance, and the Law* (Oxford: Oxford University, 1999), 16.
149. Ibid. 175
150. Ibid., 1.
151. Ibid.
152. Ibid., 15–18, 241.
153. Terry Gill and Elies van Sliedregt, *Guantánamo Bay: A Reflection on the Legal Status and Rights of 'Unlawful Enemy Combatants'*, 32, note 17.
154. Venice Commission, "Opinion on the International Legal Obligations of Council of Europe Member States in Respect of Secret Detention Facilities and Inter-State Transport of Prisoners" (Op. No. 363/2005, CDL-AD (2006)009, adopted at Venice on March 17–18, 2006), para. 78.
155. Ibid.,
156. Ibid., para. 79.
157. Christopher Greenwood, "Scope of Application of Humanitarian Law," in *The Handbook of Humanitarian Law in Armed Conflicts*, ed. Dieter Fleck, 2nd ed. (Oxford: Oxford University Press, 2008), 48.
158. Ibid.
159. Use of Force Committee, *Final Report on the Meaning of Armed Conflict in International Law*, 1.
160. Lassa Oppenheim, *II International Law: A Treatise*, edited by Hersch Lauterpacht (London: Longman, Greens, 1952), 202.
161. Use of Force Committee, *Final Report on the Meaning of Armed Conflict in International Law*, 33.
162. Ibid.
163. Use of Force Committee, *Final Report on the Meaning of Armed Conflict in International Law*, 1, 2.
164. Ibid.
165. Ibid.
166. Jean S. Pictet (ed.), *Geneva Conventions of 12 August 1949: Commentary. III Geneva Convention Relative to the Treatment of Prisoners of War: Commentary* (Geneva: International Committee of the Red Cross, 1960), 36.
167. Intensity does not depend on the subjective judgment of the parties, but it objective. See UN International Criminal Tribunal for Rwanda (ICTR), Trial Chamber I,

Prosecutor v. Akayesu, Case No. ICTR-96-4-T, judgement of September 2, 1998, para. 603. See also UN International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991 (ICTY), Trial Chamber II, *Prosecutor v. Limaj et al*., Case No. IT-03-66-T, judgment of Nov. 30,2005, para. 89.

168. *Prosecutor v. Tadić*, Case No. IT-94-1-T, opinion, and judgment of May 7, 1997, para. 562.
169. *Prosecutor v. Akayesu*, para. 620.
170. *Prosecutor v. Blagojevi and Joki*, Case No. IT-02-60-T, judgment of January 17, 2005, para. 536; *Prosecutor v. Halilovi*, Case No. IT-01-48-T, judgment of November 16, 2005, para. 24; *Prosecutor v. Limaj et al*, para. 84; *Prosecutor v. Gali*, Case No. IT-98-29-T, judgment and opinion of December 5, 2003, para. 9; *Prosecutor v. Staki*, Case No. IT-97-24-T, judgment of July 31, 2003, paras. 566–68.
171. *Prosecutor v. Mucić et al*, Case No. IT-96-21-T, judgment, November 16, 1998, para. 184.
172. See also Art. 50(2) of the *Geneva Convention (IV) of 1949*; Art. 77(2) of the *Additional Protocol I of 1977*; Art. 4(3)(c) of the *Additional Protocol II of 1977*; Art. 38(3) of the *Convention on the Rights of the Child* of 1989; Art. 4 and 8(2)(b)(xxvi)(e)(vii) of the ICC Statute of 1998; Art. 1 of the *Convention on the Worst Forms of Child Labour* of 1999; *Optional Protocol on the Involvement of Children in Armed Conflict* of 2000.