The ITPCM
International Commentary

Vol. XIII no. 39
July 2015

‘RECENT CHALLENGES TO THE INTERNATIONAL COMMUNITY: INNOVATIVE IDEAS ON HOW TO DEAL WITH THEM’

The ITPCM
International Commentary

Contributors to this issue
Andrea de Guttry, Ameneh Dehshiri,
Shisong Jiang, Rossella Marangio, Priya Sara Mathews,
Luca Raineri, Gergana Tzvetkova, Silvia Venier, Denise Venturi,
Afua Boatemaa Yakohene, Ali Al-Bayati

ISSN. 2239-7949

Scuola Superiore
Sant'Anna
di Studi Universitari e di Perfezionamento

International Training Programme
for Conflict Management
1995-2015, 20th Anniversary

International Commentary

Vol. XIII no. 39 JULY 2015 ISSN. 2239-7949

‘RECENT CHALLENGES TO THE INTERNATIONAL COMMUNITY: INNOVATIVE IDEAS ON HOW TO DEAL WITH THEM’

Newly launched on the ITPCM agenda:

Next Events & Trainings, more at p. 64

Table of Contents

PRESENTATION OF THIS ITPCM COMMENTARY ISSUE

Andrea de Guttry
Full Professor of Public International Law & Director,
International Training Programme for Conflict Management, Scuola Superiore Sant'Anna

Dear friends and readers of the ITPCM Commentary,
I am very pleased to send to all of you our warmest greetings from a very warm Pisa.

Recent events related to terrorism, violent attacks, mass immigrations, IDPs, civil and international wars, organised crime, economic and financial crises etc. need to be urgently addressed in a more structured way, through a higher level of cooperation and coordination among the States, with a specific attention to the respect of human rights and with a more active role played by relevant international organizations (both at universal and at regional level). What is urgently requested is, as well, a more comprehensive and long term approach in dealing with these challenges.
There have been interesting steps in this direction, especially to counter the phenomenon of foreign fighters which has been high on the agenda in the last months. UNSC Resolution 2178 (2014) represents an interesting case as the Council underlined the importance of Member States' efforts to" develop non-violent alternative avenues for conflict prevention and resolution by affected individuals and local communities to decrease the risk of radicalization to terrorism, and of efforts to promote peaceful alternatives to violent narratives espoused by foreign terrorist fighters, and underscores the role education can play in countering terrorist narratives".
As a public University and as peace-loving citizens we have to play an important role and we cannot continue to hide ourselves hoping that others will do what needs to be urgently done.
Against this framework, this issue of our ITPCM Commentary is almost entirely devoted to analyze and debate a few relevant challenges the International Community is facing nowadays. Issues such as cyber attacks, nuclear cyber security, the security–development nexus, organised crime and peace operations, the role of resilience in dealing with terrorism events, foreign fighters, protection of the LGBT's right when applying for refugee status, the role of Boko Haram and finally a few specific dilemmas Independent High Electoral Commissions are facing, are addressed in the contributions you will find in this issue.
I really hope that we will be able to shed some light on issues which are neglected or, in any case, deserve more attention by the public opinion and decision makers worldwide. I am very grateful to all contributors and to the Editorial Committee who has carried out a tremendous job.

In the second part of the ITPCM Newsletter you will find, as usual, additional info on new training courses which we are planning to deliver in 2015: you will notice that we are expanding the topics of these courses and trying to make them more and more focused on the specific needs of those serving in international field operations.

As the next issue of our Commentary is due to appear in December 2015, we would to warmly invite all of you to send us short contributions about the activities you are carrying out or about specific issues you are dealing with: these contributions will make our Commentary more appealing and vivid.

I wish to all of you and your families all the best and a wonderful Summer

Andrea de Guttry

APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW ON ISOLATED CYBER NETWORK ATTACKS

Ameneh Dehshiri
Ph.D Candidate in International Law
Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
a.deshiri@sssup.it

Abstract

Information and communication technology changed the way we live, learn and even fight. Information is not only a military supplementary means anymore, but a target itself. Computer network attacks (CNAs) are able to make widespread destruction and human injury in reality. But the question is whether CNAs conducted by one State against another can be the subject of international humanitarian law. This paper seeks to address the legal situation of CNAs which are not operated in the context of a current ongoing combat.

Keywords

Cyber network attack, International humanitarian law, international armed conflict, armed force, attribution.

1. Cyber world, cyber war: an Introduction

Internet technology has changed the way the world operates. (Joyner and Lotrionte, 2001) The word 'cyberspace' is often applied to activities, communications and relationships made possible by the Internet. (Rowland, 2011) Cyberspace has been defined as "a geographically unlimited, non-physical space, in which- independent of time, distance and location - transactions take place between people, between computers and between people and computers". (Hamelink, 2000) Cyberspace has pervaded in our every day activities. In like manner, control and operation of key infrastructure in economic social, political, energy and military activities increasingly relies upon information and telecommunications technology. (Hollis, 2007) This interlinked world even changed the strategy and methods of warfare.

The control of information has always been a key element in war. (Haslam, 2000) Nowadays, however, information and information infrastructure is a target itself rather than a mean to achieve other military objectives. (Kanuck, 1996) Cyber Network Attacks (CNAs) are using "networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." (Poisel, 2013, 37) A symbol of this new era is a malicious software worm dubbed "Stuxnet." In 2010, Stuxnet stuck in an Iranian nuclear facility at Natanz. Actually malicious software has been with us for more than 25 years, but Stuxnet was unlike any other virus or worm that came before. Rather than hijacking targeted computers or stealing information from them, it was aimed to cause physical destruction on equipment the computers controlled. Stuxnet was described as the first demonstration of the capability of software to have malicious physical effect in the real world. (Zetter, 2014) Before the development of Stuxnet many experts in cyber conflicts believed "cyber war only kills a punch of little baby electrons." Stuxnet showed the world that cyber war could potentially kill real babies. (Poisel, 2013, 2) Neither Israel nor the United States have publicly acknowledged being behind Stuxnet, but anonymous U.S. national security officials have told news outlets that the two countries worked together to launch the attack. This instance rise awareness in the reality of cyber warfare domain.(Waterman, 2013)

Therefore, CNAs are able to inflict a wide range of damage immediately. (Korzak, 2014, 151) A major legal debate with regard to CNAs emerged around the applicability of international humanitarian law (IHL). (Schmitt, 2002) According to Geneva Convention the applicability of IHL based on the existence of an armed conflict.(*Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, 1949 article 2) The difficult situation, with regard to applicability of IHL, is where CNA is the first or the only malicious action. (Haslam, 2000; Schmitt, 2002) CNAs do not involve violence directly and do not easily fit within established category of "armed conflict", "armed force" and "armed attack." Despite some calls for drafting a new convention to address the issues raised by CNAs, (Brown, 2006; Hollis, 2007) many authors believe that this is unnecessary. According to them existing laws are capable of adapting to the new technology.(Kueh, 2002; Schmitt, 2002)

This paper seeks to identify important questions associated with application of IHL on isolated cyber attack (such as Stuxnet) which is trigged by state against another one. Therefore, a discussion of non international armed conflicts falls outside the scope of this paper.

2. Applicability of International humanitarian law (IHL)

IHL "shall apply to all cases of declared war or of any other armed conflict which may arise between

two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."(*Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, 1949 Article 2) IHL governs conduct during wartime and provide overall framework for conduct of hostilities and the protection of persons and objects. (Yingling and Ginnane, 1952) Under the provisions of the Geneva Conventions and Additional Protocols some of the fundamental principles of IHL are:

- Military necessity: military operations must serve a concrete military purpose (*Additional Protocol I*, 1977 Articles 48,51(2), 52);
- Distinction principle: parties to a conflict must distinguish between civilians and combatants and between civilian objects and military targets (*Additional Protocol I*, 1977 Article 51(4), (5));
- Proportionality: injury to civilians or damage to civilian objects must not be disproportionate to the anticipated military advantage (*Additional Protocol I*, 1977 Article 57).

In brief, these principles are mandating that: 1) the civilians "shall enjoy general protection against dangers arising from military operation," and 2) the civilians "shall not be the object of attack." (*Additional Protocol I*, 1977 Article 51 (1) and (2)) these rules are derived from the principle of distinction, which mandate that parties to a conflict must distinguish between those who are fighting and those who are not and only target attacks at the fighters. (*Additional Protocol I*, 1977 article 48) What is relevant here is the definition of attack during an armed conflict. There are significant differences between the notion of attack in IHL from the one in *jus as bellum*:

1. Protocol commentary indicates that Attack in IHL is entirely different from the notion of "Armed attack" in jus as bellum: "finally it is appropriate to note that in the sense of the Protocol an attack in unrelated to the concept of aggression or the first use of armed force; it refers simply to the use of armed force to carry out a military operation at the beginning or during the course of an armed conflict. Questions relating to the responsibility for unleashing the conflict are of a completely different nature." (Pilloud et al., 1987, 603)

2. Not all actions of a military or other parties to a conflict will constitute attack. Under IHL, military operations and attack are distinguished. For example, "nondestructive psychological operations directed at the civilian population, such as dropping leaflet, broad casting to the enemy population, or even jamming enemy public broadcasts " all are military operation but do not meet the definition of attack under IHL. (Schmitt, 2012) Attack in IHL applies to both offensive and defensive act and involves violence or combat action. (Pilloud et al., 1987, p. 603) Conventional conflicts encompass traditional means such as means and warfare, such as bombing, shelling, or the deployment of troops. Therefore, "armed force" that has the direct descriptive effect on property and persons becomes widely used to a delicate IHL application. (Droege, 2012) For example, In the words of the International Criminal Tribunal for the former Yugoslavia (ICTY), in Tadic case, an international armed conflict arises "whenever there is a resort

to armed force between States." (*Prosecutor v. Tadic*, 1995, para. 70) Article 51 of Additional Protocol I declared that the concept of attack includes violent acts against enemy personnel or object as well as violent acts against civilians. "The term 'act of violence' denotes physical force. Thus the concept of 'attack' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare." (Bothe et al., 1982)

The 'Instrumental based approach' and the 'consequence-based approach' are two approaches that are used for interpreting the notion of armed force. Under the instrumental based approach the criterion of violence is limited to the method of attack. Thus, we simply ask whether force has been used. (Schmitt, 1999) But, in the consequence-based approach for identifying an armed attack the means are not important *per se*. Whenever "the consequences of the attack are equivalent to damage done by traditional weapons" the armed attack excites. (Hanseman, 1997)

Under the current consequence-based approach our attention would shift from the instrument of armed force to the effect of their employment. The direct consequence of using armed force is physical destruction and injury. (Joyner and Lotrionte, 2001) This explains why the use of biological, chemical, and radiological weapon constitute attacks even though they do not use physical force. (*Prosecutor v. Tadic*, 1995) Additional Protocol I also focuses on the effects of attacks on the civilian population and on civilian objects, on dangers to civilians and other harms that are identified by the consequence of an act rather that the nature of the act itself. (Bothe et al., 1982; Droege, 2012; Schmitt, 2013).

3. Armed conflict and CNAs

As mentioned, IHL only applies to a specific set of state behavior involving "armed conflict." Therefore, CNAs must occur "in the context of and related to an armed conflict" in order to be regulated by IHL. (Droege, 2012) If CNAs arise in the context of a conventional armed conflict there will be no barriers for the application of IHL on them. For instance, there was an armed conflict between Georgia and Russia, in 2008. During the conflict, Russia launched a cyber attack on the computer systems of its adversary. In this case, two states already are involved and engaged in an act amounting to armed force. (Schmitt, 2013 Rule 20(3)) Special difficulty arises where States engage in an isolated CNA as the only malicious operation. The question is whether "isolated" CNAs that are not accompanied by conventional conflict attacks would be considered as the subject of IHL. Two particular challenges make the identification of an armed conflict difficult in a solely armed conflict: whether the damage is sufficient to qualify CNA as "armed force" and whether it is possible to attribute the CNA to a state.

As discussed earlier, the term of 'attack' in IHL refers to "the use of armed force to carry out operation at the beginning or during the course of an armed conflict." (*Additional Protocol I*, 1977) Here, concept of attack includes violent acts against enemy personnel or object as well as violent acts against civilians. The key elements are intent and likely result of an attack, "not the novel method of attack."(Scott, 1998)

CNAs contain a particular challenge for the definition of attack because cyber acts do not involve violence directly. Such operations may end up with violence effects, but the act itself is not violent in the way that the operation involves violence. The Tallinn Manual[1] defines CNA as "cyber operation whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."(Schmitt, 2013 Rule 30) It can thus be suggested that the consequences of a CNA determine whether a cyber operation constitute an attack. As defined in Article 49 of Additional Protocol I, (*Additional Protocol I*, 1977 Article 49) CNAs that cause consequential damages to individuals or objects, or interfere in the functionality of an object, will meet the threshold for and attack. (Schmitt, 2013 Rule 30)

Knut Dörmann, the Deputy Head of the Legal Division in International Committee of the Red Cross, indicates that the CNAs can be characterized in the IHL as a "cyber operation by means of viruses, worm, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked" (Dörmann, 2004)

Schmitt also points out:

"Humanitarian law principles apply whenever CNAs can be ascribed to a State, are more that merely sporadic and isolated incidents, are either intended to cause inquiry, death, damage or destruction (and analogous effects), or such consequences are foreseeable. This is so even though classic armed force is not being employed." (Schmitt, 2002)

Whenever the CAN would not meet the above-mentioned criteria, IHL principles are not applicable. This condition might be in contrast with the purpose of IHL, since the purpose of IHL is limiting damage resulting from hostilities and to protect civilians and civilian objects from attacks. Also some authors have pointed out that this interpretation can lead to creation of a "grey area" that is not covered by IHL. It could indeed increase the possibility of targeting civilian objects by CNAs in a way that do not result to injury or destruction. In this way CANs

[1] The Tallinn Manual is the product of a three-year project by twenty renowned international law scholars and practitioners, the Tallinn Manual identifies the international law applicable to cyber warfare and sets out ninety-five 'black-letter rules' governing such conflicts. It addresses topics including sovereignty, State responsibility, the jus ad bellum, international humanitarian law, 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.

fall outs of established categories and can conducted without the legal restriction of necessity, distinction and proportionality. (Korzak, 2014, p. 158)
To make an example, a country's banking system or national data trafficking might be manipulated without any of physical damage. (Droege, 2012) Hollis warn about the threat of this kind of interpretation and argues:
"The irony of IO [information operation] is that the less likely it is that a particular information operation function as an attack, the more likely it is that it use against civilians and their objects is permissible."(Hollis, 2007)
In this way the interpretation of armed conflict and armed force in CNAs scale could lead to some challenges that need to be considered by scholars. Still, other bodies of law such as jus ad bellum, cyber crime law, cyberspace law, telecommunications law and human rights law might apply in "grey area" and provide their own protection.

4. Attribution of CNAs to State

In IHL attribution encompasses the issue of who carried out an attack. The attacker attribution goes to assign responsibility for committing an attack. Finding the origin of cyber attack in a borderless space is not easy. Even if technology tracks the attack to a single computer of number of computers, still we cannot say from where the attack has originated. Computers of ordinary users might be controlled by hackers for launching CNAs. These remote controls are not restricted to territorial boundaries. (Lin, 2012)
In traditional conflicts the attack was conducted by military forces that are presumed to be under the control of national governments. (*Nicaragua v. United States of America*, 1986) No such presumption governs the actors participating in cyber conflict, and definitive attribution of acts in cyberspace to national governments is very difficult or impossible. The signals bear neither state insignia nor other markers of military allegiance or intent. (Brenner, 2008, 425) The Tallinn Manual takes a similar legal view in Rule 7:
"The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation". (Schmitt, 2013)
Without identifying the parties as two or more States it is impossible to classify the situation as an international armed conflict. In practice some technical measures can be applied to make the CAN attributable to a particular state, and this method is based on all the available sources of information. (Droege, 2012) In addition, human intelligence might provide critical information about the location of the system that launched a CNA. (Lin, 2012).

5. Conclusion

CNAs do not involve violence directly and do not easily fit within established categories of "armed conflict", "armed force" and "armed attack." However, such operations may end up having violent effects. If there is a reasonable expectation for the CNA "to cause injury or death to persons or damage or destruction to object", then it would constitute an attack under the notion of IHL. (Schmitt, 2013 Rule 30)
After meeting the mentioned threshold, IHL legal constraints are applicable on CNAs, even where it is the first or the only malicious action conducted by a State against another State. By application of IHL legal constraints, CANs may only be undertaken to the degree and in a way respecting the existing law.
- CNAs must be only against "military objectives" and not to attack civilians or civilian objects; (*Additional Protocol I*, 1977 Articles 48, 51 (2), 52)
- If after the assessment any methods of CNAs are recognized as inherently indiscriminate (such as worm viruses) they would be illegal weapons according to IHL and thus banned; (*Additional Protocol I*, 1977 Article 51 (4), (5))
- Incidental civilian damage of CNAs must be minimized. When damage of CNAs is likely to be excessive to the value of the military objective to be attacked state has an obligation to abstain from attacks. (*Additional Protocol I*, 1977 Articles 51 (5)(b), 57 (2)(a)(ii) and (iii))

References

Bothe, M., Partsch, K.J., Solf, W., 1982. New rules for victims of armed conflicts. Terminol. B 8, 9.

Brenner, S.W., 2008. Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford University Press.

Brown, D., 2006. Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, A. Harv Intl LJ 47, 179.

Dörmann, K., 2004. Applicability of the Additional Protocols to computer network attacks.

Droege, C., 2012. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. Int. Rev. Red Cross 94, 533–578.

Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 1949. . International Committee of the Red Cross.

Hamelink, C.J., 2000. The ethics of cyberspace. Sage.

Hanseman, R.G., 1997. The Realities and Legalities of Information Warfare. Air Force Law Rev. 173–184.

Haslam, E., 2000. Information warfare: technological changes and international law. J Confl. Sec L 5, 157.

Hollis, D.B., 2007. Why states need an international law for information operations. Lewis Clark Law Rev. 11, 1023.

Joyner, C.C., Lotrionte, C., 2001. Information Warfare as International Coercion: Elements of a Legal Framework. Eur. J. Int. Law 12, 825–865.

Kanuck, S.P., 1996. Information Warefare: New Challenges for Public International Law. Harv Intl LJ 37, 272–568.

Korzak, E., 2014. Computer network attacks, self-defence and international, in: Hehir, A., Kuhrt, N., Mumford, A. (Eds.), International Law, Security and Ethics: Policy Challenges in the Post-9/11 World. Routledge, pp. 147–164.

Kueh, D.T., 2002. Information Operations, Information Warfare, and Computer Network Attack—Their Relationship to National Security, in: Schmitt, M.N., O'Donnell, B.T., (U.S.), N.W.C. (Eds.), Computer Network Attack and International Law. Naval War College.

Lin, H., 2012. Cyber conflict and international humanitarian law. Int. Rev. Red Cross 94, 515–531.

Nicaragua v. United States of America, 1986.

Pilloud, C., Sandoz, Y., Swinarski, C., Zimmermann, B., 1987. Commentary on the Additional Protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949. Martinus Nijhoff Publishers.

Poisel, R.A., 2013. Information Warfare and Electronic Warfare Systems. Artech House.

Prosecutor v. Tadic, 1995.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977. International Committee of the Red Cross.

Rowland, D., 2011. Virtual World, Real Rights? Human Rights and the Internet, in: Emerging Areas of Human Rights in the 21st Century: The Role of the Universal Declaration of Human Rights. pp. 7–23.

Schmitt, M., 2012. "Attack" as a term of art in international law: The cyber operations context, in: Cyber Conflict (CYCON), 2012 4th International Conference on. IEEE, pp. 1–11.

Schmitt, M.N., 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Schmitt, M.N., 2002. Wired warfare: Computer network attack and jus in bello. Rev. Int. Croix-Rouge International Rev. Red Cross 84, 365–399.

Schmitt, M.N., 1999. Computer network attack and the use of force in international law: thoughts on a normative framework. Columbia J. Transnatl. Law 37, 1998–99.

Scott, R.D., 1998. Legal aspects of information warfare: military disruption of telecommunications. Nav. Rev 45, 57.

Waterman, S., 2013. U.S.-Israeli cyberattack on Iran was "act of force," NATO study found [WWW Document]. Washington Times. URL http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/ (accessed 6.9.15).

Yingling, R.T., Ginnane, R.W., 1952. The Geneva Conventions of 1949. Am. J. Int. Law 393-427.

Zetter, K., 2014. An Unprecedented Look at Stuxnet, the World's First Digital Weapon [WWW Document]. WIRED. URL http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed 7.1.15).

APPLYING INTERNATIONAL LAW TO ADDRESS THE EMERGING CHALLENGE OF NUCLEAR CYBER SECURITY: OVERVIEW, REFLECTION AND PROSPECT

Shisong Jiang
Ph.D Candidate in International Law
Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
s.jiang@sssup.it

Abstract

This article assesses the existing international legal framework with respect to the emerging cyber-security related challenges in the nuclear security field. By briefly outlining the international legal basis of nuclear security, it aims at uncovering the main possible "entrances" of the current international nuclear security framework for cyber security. Accordingly, some critical reflections and corresponding suggestions are provided and discussed afterward.

Keywords

Nuclear security, cyber security, international nuclear security law, International Atomic Energy Agency (IAEA).

1. Introduction

Whereas there has been a rapid development of nuclear science and technology all over the world, nuclear security issues have been correspondingly upgraded as a top-priority theme in the international community agenda[1]. From both the military and civilian perspectives, nuclear and other radioactive materials are increasingly associated with various risks due to the potential to cause damage on a large scale. Apart from the consistently great efforts being made by the international community in order to guarantee nuclear safeguards and nuclear safety, nuclear security has gradually occupied the central stage during the last decade, although the inadequacy of efforts is rather salient compared with the former two areas[2]. Its dominant position in the international affairs has been kept reinforcing especially in the general context of global tide of anti-terrorism after the 9/11. Not only have states started to take substantial actions to secure their nuclear materials at domestic level[3], but also certain consensus on the need for global governance of nuclear security has also been reached at the international level.

In contemporary times, one of the main challenges for nuclear security is related to the emerging threat of cyber attacks (Hathaway 2012). Thanks to the so-called digital revolution, Information and Communication Technology (ICT) have swiftly expanded their sphere of influence to critical infrastructures (Brocklehurst 2015), including nuclear power plants. Increasing numbers of analog systems have been replaced by digital control systems, which mainly accessorize with computer networks composed by commercial off-the-shelf operating system (including hardware and software) (Kesler 2011). For instance, Windows is one of the most typical systems employed by nuclear power plants. Although this technological shift has widely facilitated the nuclear facility management and in particular the remote management, vulnerabilities of nuclear security induced by cyber attacks over the internet have been identified (Kesler 2011). For sure, A cyber attack has an actual impact on nuclear security, as it has been broadly recognized by the international community especially after the Iranian centrifuges at Natanz were intentionally attacked by the offensive Stuxnet malware in 2010 (BBC NEWS 2010). Indeed, distinctive scenarios reflecting the serious risks to nuclear security are underlying the cyber threat (Dudenhoeffer 2013)[4]. It indicates that the targets of cyber attack are not limited to the nuclear or other radioactive materials, the

nuclear facility itself, but they also include sensitive nuclear information etc.

As a global challenge, the international legal regime has inadequately made contribution to the nuclear security governance. As a matter of fact, legal methods have not been considered as the priority to address the nuclear security issues partially because of the state sovereignty and national security strategy among states. Therefore, compared with the legal methods, political efforts and commitments have played a more significant role. However, this does not mean to distort the appreciation of the existing international legal framework for nuclear security. Then, the crucial question is whether the emerging nuclear cyber security issues, instead of referring to other more general international legal framework[5], can be specifically addressed by the international legal framework of nuclear security[6]. This paper aims to analyse this question by reviewing the overall structure of the international nuclear security law in section 2. In Section 3 the paper tries to explain where cyber security fits into the current international nuclear security framework. Eventually, some reflections and prospects on the international legal framework for nuclear cyber security are discussed in section 4.

[1] For instance, the World Economic Forum has specific Global Agenda Council on Nuclear Security in order to "merge traditional voices of nuclear security with industry voices, providing the ideal environment to lead discussions on these issues." See more on http://www.weforum.org/content/global-agenda-council-nuclear-security-2014-2016-0 [Accessed 2 May 2015].

[2] The current international nuclear regime mainly includes nuclear safeguard, nuclear safety and nuclear security. The nuclear safeguards refer to a system of inspection and verification of the peaceful uses of nuclear materials as part of the Nuclear Non-Proliferation Treaty (NPT). The nuclear safety means the achievement of proper operating condition, prevention of accidents and mitigation of accident consequences, resulting in protection of worker and the general public from dangers arising from ionizing radiations from nuclear installations. For nuclear security, it is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. Available from http://www-ns.iaea.org/standards/concepts-terms.asp [Accessed 16 May 2015].

[3] United States Nuclear Regulatory Commission, for example, has adopted series of regulations and other administrative actions for protecting people and the environment. See more on http://www.nrc.gov/ [Accessed 25 April 2015].

[4] IAEA has identified three significant risk scenarios involving cyber attacks on civil nuclear facilities. First, a cyber attack that causes the unauthorized removal of nuclear or another radioactive materials; Second, cyber sabotage that affects the normal functioning of a nuclear facilities or other parts of the nuclear fuel cycle; Third, cyber espionage that results in the collection and exploitation of sensitive nuclear information.

[5] For instance, the Convention on Cybercrime (2004) and its Additional Protocol (2006).

[6] There was an International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange on 1-5 June 2015 which demonstrates the great importance of this topic. See more on: http://www-pub.iaea.org/iaeameetings/46530/International-Conference-on-Computer-Security-in-a-Nuclear-World-Expert-Discussion-and-Exchange [Accessed 12 June 2015].

2. Overview of international nuclear security law

International nuclear law[7], as a branch of international law, has been initiated since the 1950s on the basis of the breakthrough of atomic technology as well as of its trans-boundary and potentially disastrous consequences. The International Atomic Energy Agency (IAEA), founded in 1957, is the most important intergovernmental organisation aiming at both promoting the development of nuclear science and technology and preventing human beings from the potential hazards associated therewith by leading to the construction of a transnational legal architecture in this field. Pursuant to IAEA's mandate endowed by its statute[8], the triangle structure of international nuclear law has been gradually formulated as being composed of nuclear safeguards, nuclear safety and nuclear security. Thus, a number of international legal instruments have been used for the purpose of comprehensively regulating these three separated but correlated fields.

However, not until the early 1970s the IAEA has been requested to engage in strengthening the international mechanism of nuclear security under the circumstances of a growing necessity for 'cooperation among States to ensure the physical protection of nuclear material against theft or unauthorized removal, especially during international transport, and against the sabotage of nuclear facilities' (IAEA 2011 3). In addition to the usual physical protection of nuclear materials, IAEA has expanded its attention to combat nuclear terrorism after the 9/11 terrorist attacks. The events of 9/11 were also the occasion for the international community to reflect on the threats posed by cyber attacks, included 'among the threats that nuclear plants would be required to defend against' (Holt & Andrews 2014 11). To that end, IAEA has begun to undertake series of actions to provide States with the necessary guidance and external expertise by issuing for instance the Nuclear Security Series Documents[9].

There are several international legal instruments with respect to nuclear security. The main treaties[10] are the Convention on the Physical Protection of Nuclear Material (CPPNM) and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT). The CPPNM, which was adopted on 26 October 1979 and entered into force on 8 February 1987, is the only legally binding document at the international level devoted to the physical protection of nuclear material. In order to broaden its scope and thereby strengthen the international physical protection regime, especially in terms of reducing the vulnerability to nuclear terrorism, the Amendment of the CPPNM was adopted on 8 July 2005. However, because of the low number of ratification by State Parties, the Amendment has not entered into force so far. As to the nuclear terrorism, the ICSANT is explicitly seeking to prevent and punish relevant acts. Furthermore, United Nations (UN) Security Council Resolution 1373 (2001) and Resolution 1540 (2004) have required increasingly importance to the international legal regime for nuclear security. Meanwhile, it is noteworthy that there are several provisions regarding nuclear security in the nuclear-related treaties[11].

3. Where does cyber security fit into the current international nuclear security framework?

It is, however, impossible to find any reference to 'cyber security' in the aforementioned legally binding documents. The cyber security

[7] The nuclear law here (Stoiber 2003) refers to 'the body of special legal norms created to regulate the conduct of legal or nature persons engaged in activities related to fissionable materials, ionizing radiation and exposure to natural sources of radiation'.

[8] Article II of Statute states that the IAEA is to accelerate and enlarge the contribution of atomic energy of atomic energy to peace, health and prosperity throughout the world. Available from https://www.iaea.org/about/statute [Accessed 18 May 2015].

[9] See the Nuclear Security Series Publications in http://www-ns.iaea.org/security/nss-publications.asp [Accessed 11 May 2015].

[10] Conventions here refer to the specific ones for nuclear security under the auspices of IAEA. Apart from these conventions mentioned here, there are other conventions have connection (direct or indirect) with nuclear security. For instance, under the auspices of the International Maritime Organization, there is The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1998), The 2005 Protocol to the SUA Convention, etc.

[11] For instance, Central Asia Nuclear Weapon Free Zone Treaty (2008), Pelindaba Treaty for Africa (2009), Tlatelolco Treaty for Latin America (1968), etc.

threats that are relevant to nuclear security have been mainly addressed through non-binding instrument at the international level. The non-binding instruments, as international soft law, are actually applicable to the nuclear power plants and other facilities. Specifically, since IAEA plays a leading role with regard to the legal regulation on the peaceful use of nuclear energy, it is also the primary actor for international soft law on nuclear cyber security. Generally speaking, IAEA has constantly issued Nuclear Security Series (NSS), including categories of Nuclear Security Fundamentals, Nuclear Security Recommendations, Implementing Guides and Technical Guidance, although its mandate does not explicitly permit the promulgation of security "standards" (IAEA 2011). In particular, the comprehensive methods regarding nuclear security issues are specifically reflected in NSS No. 13, 14, 15 and 20. Due to the political sensitivity of the nuclear cyber security area, IAEA has persistently been requested 'to raise awareness of the threat of cyber attack and their potential impact on nuclear security' (IAEA 2013). To achieve this, IAEA has published a number of documents to 'build a top to bottom framework to support Member States, Competent Authorities, and nuclear organizations in developing and conducting assurance activities for computer security' (Mrabit 2014: 7). Accordingly, it is possible to simplify the international soft law framework of nuclear cyber security as (Dudenhoeffer 2013):

Nuclear Security Fundamentals

- NNS No. 20, Objective and Essential Elements of a State's Nuclear Security Regime.

Nuclear Security Recommendations

- NSS No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities.
- NSS No. 14, Nuclear Security Recommendation on Radioactive Material and Associated Facilities

Implementing Guides

- NSS XXX Information Security: Protection and Confidentiality of Sensitive Information in Nuclear Security.

Technical Guidance

- NSS No. 17, Computer Security for Nuclear Facilities.
- Conducting Computer Security Incident Investigation and Forensics at Nuclear/Radiology Facilities.
- Computer Security Incident Response Exercises for Nuclear/ Radiological Facilities.
- Cyber Security Regulation.
- Conducting Computer Security Assessments for Nuclear Facilities.
- Applying Computer Security Controls to Instrumentation and Control Systems at Nuclear Facilities
- Incident Response Planning for Computer Security Events at Nuclear/ Radiological Facilities.

Additionally, IAEA is still working on new drafts regarding the nuclear cyber security[12]. In all, these non-binding documents may result in the integration of the cyber security issues within the institutional mechanism of international nuclear security through the continuous constructions of soft law.

The associated legal methods associated with the nuclear cyber security have been developed and implemented according to some specific features. First and foremost, the most remarkable trait is the fact that soft law is now dominating the regulation of international nuclear cyber security. Compared with reaching international legal commitments through a complicated procedure, soft law does provide more flexibility (Guzman & Meyer 2011). Especially when a new concern emerges, the nuclear cyber security is prompter in replying to the related regulatory needs from the international perspective. Of course, the sensitivity of nuclear issues and of nuclear weapons in particular is not deniable. It is, therefore, in this regard that these non-binding instruments are able to fill the lacuna of political uncertainties from both the nuclear and the cyberspace side. In fact, an increasing number of states are implementing IAEA's documents with respect to the hybridity of nuclear and cyber security in the domestic level through legislation and/or policy.

Second, the current international legal framework on nuclear cyber security is monopolised by IAEA' non-binding documents, i.e. the international community intends to insert the nuclear cyber security issues into the general nuclear security framework rather than dealing with it through the general cyber security framework. Accordingly, IAEA's position regarding cyber security regime is indispensably critical; practice actually proves this. Apart from publishing nuclear security documents, IAEA runs a particular cyber security programme in the Office of Nuclear Security 'designed to provide states with necessary guidance and external expertise to detect and respond to cyber attacks involving nuclear or radioactive material and associated facilities' (Boulanin and Ogilvie-White 2014). Moreover, IAEA facilitates nuclear cyber security information exchange by establishing a dedicated cyber security section in the IAEA Nuclear Security Information Portal. Furthermore, IAEA provides nuclear cyber security training programmes, expert support and services to distinctive regions and states. All of these activities are consistent with the concrete content of the international soft law regime which has tried to intangibly construct an IAEA-centered international regime of nuclear cyber security.

[12] For instance, the Computer Security of Instrumentation and Control Systems at Nuclear Facilities (NST036), was welcoming comments until 17 April 2015. See http://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst036.pdf [Accessed 15 May 2015].

4. Reflection and prospect on the international legal framework for nuclear cyber security

The international legal framework of nuclear cyber security is intertwined with various shortcomings. Among the flaws, the legal effect of international soft law regulating the cyber threat to nuclear vulnerabilities is frequently criticised. Even though flexibility may be an asset, on the other hand it can be an issue. IAEA's nuclear security publications are not binding documents so that international legal obligations are not formulated at all. Without international legal obligations, states may be more reluctant to implement international standards at domestic level. Although there are states voluntarily referring to these non-binding documents and actively participating in this international regime, many states at present seem to lack the political will, capacity and/or security culture to do so. Certainly, this status quo is not compatible with the consequential severity and strategic significance of the current or potential cyber threat to nuclear security.

The non-binding attribute, unfortunately, is not the only flaw of the existing legal framework, which may be also criticised from the point of view of its actual content. First of all, it is inevitable to keep in mind the institutional deficiency of the general legal framework of nuclear security. Differently from the area of nuclear safety, the current international nuclear security instruments do not include the monitoring and enforcement structures needed to ensure accountability and to provide confidence in the effective implementation of strong security measures across borders. Thus, some instrument of this legal regime (for instance, assessment, information sharing and peer review), are missing from the general nuclear security framework too, therefore they are not included in the nuclear cyber security. In light of the integral inadequacy of hard law to address the nuclear cyber issues, provisions emanated from soft law are still not enough. Critically speaking, IAEA's instruments are mainly focusing on the information and computer security in a narrow sense, but the cyber security is not limited to them obviously. As to the content, information cooperation and assessment are the cornerstones of these documents, which need to be broadened for a larger sense.

Simultaneously, criticisms have emerged with respect to the nuclear security regime which is regarded as the logical consequence of the legal framework flaws described in the previous paragraphs. Skeptics have already claimed that 'there is no uniformity in the nuclear security regime today and this creates vulnerabilities[13]. Given the mandate IAEA has in the nuclear security field, its actions, on the one hand, are not as effective compared to the actions regarding nuclear safety. On the other hand, IAEA actually has been more or less marginalised especially in dealing with enhancing the international cooperation of nuclear security in recent years. Conversely, the Nuclear Security Summit[14] has become more efficient as a provisional mechanism which partially demonstrates that the international community is still not confident in the institutional arrangement under IAEA. Although the Nuclear Security Summits both in Seoul (2012) and The Hague (2014) emphasised the need for action in the area of information and cyber security, the current international regime is not able to address these issues, in particular as a result of the IAEA's feeble non-binding instruments.

As discussed above, the existing international legal framework of nuclear security is not sufficient to address the emerging cyber threats. It is therefore a vital task to coordinate the two thematic areas in one unified system in the future. Whereas the sensitivity of nuclear and other radioactive materials IS dealt with great political attention, there are possibilities to adjust the applicable international legal framework. The notion of cyber security shall be reflected in the existing conventions by different means. The broader interpretation of the nuclear security to include cyber security is going to facilitate its entry to the presented framework. It could be a great opportunity to negotiate this on the occasion of pushing the entry into force of the CPPNM Amendment. However, the ideal scenario would be the adoption of a specific convention, namely the International Convention on Nuclear Security as proposed recently[15], to comprehensively regulate cyber security issues within the general structure of nuclear security. In this case, the international legal instruments for nuclear safety is going to be a model, which means that the nuclear cyber security framework must include provisions with respect to the monitoring mechanism on the basis of the international legal obligations.

Considering the fact that non-binding documents are the primary component of the international regime of nuclear cyber security, it is necessary to seriously take them into account from different points of view. The transformation from soft law to hard law will be one direction of IAEA's further endeavour (Bailliet 2012). This, however, would be only possible on the premise of the extensive implementation of these documents. Thus, IAEA will play an even more important role in the international nuclear security regime. This will make sense especially when the international community is standing at crossroads

[13] The nuclear security regime is typically understood to comprise domestic laws and regulations that govern security within a country's territory; international agreements, institutions, and UN resolution that supplement national laws; and ad hoc, cooperative measures in which countries voluntarily participate.

[14] The Nuclear Security Summit is a world summit, aimed at preventing nuclear terrorism around the globe. See http://www.state.gov/t/isn/nuclearsecuritysummit/index.htm [Accessed 29 June 2015].

[15] International Convention on Nuclear Security (2015). Available from: http://www.nsgeg.org/ICNSReport315.pdf [Accessed 4 May 2015].

of the potential ending of the Nuclear Security Summit in 2016. Then, instead of completing the entire regime, it will not be possible to realise the global governance of nuclear cyber security by solely adjusting the law.

5. Conclusion

Securing cyberspace is extremely critical for the final goal of nuclear security both from the technological and institutional perspectives. As this brief analysis pointed out, the main challenge for nuclear cyber security at present is related to the over-reliance on the non-binding instruments of the general international nuclear security framework. States' political commitments to take serious international legal obligations to address the actual cyber attacks and to reduce the potential cyber risks are apparently lacking. This reality results in the vulnerability of nuclear security. In order to reverse this condition, it is time to rethink the imbalance of institutional configuration as well as the inadequacy of legal effect under the IAEA-leaded framework of international nuclear security law. Within the process, this paper argues that dealing with the non-binding instruments regarding cyber security in nuclear areas is the core that eventually will enhance the transformation of soft law to hard law. Moreover, it is the desire that thereby directs the further development of the international nuclear security law.

References

Brocklehurst, K. (2015) Cyberterrorists Attack on Critical Infrastructure Could Be Imminent. [Online] Available from: http://www.tripwire.com/state-of-security/security-data-protection/security-controls/cyberterrorists-attack-on-critical-infrastructure-could-be-imminent/ [Accessed 3 May 2015].

Boulanin, V. and Ogilvie-White, T. (2014) Cyber Threats and Nuclear Dangers. [Online] *Policy Brief No. 17*. P. 8. Available from: http://www.a-pln.org/sites/default/files/apln-analysis-docs/Policy%20Brief%20No%2017%20-%20Cyber%20Threats%20and%20Nuclear%20Dangers.pdf [Accessed 2 June 2015].

Bailliet, C. (2012) *Non-state Actors, Soft Law, and Protective Regimes: From the Margins*. New York: Cambridge University Press.

Dudenhoeffer, D. (2013) Office of Nuclear Security: Cyber Security Programme. [Online] IAEA, PowerPoint Presentation. Available from: https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf [Accessed 2 June 2015].

Guzman, A.T. and Meyer, T. (2011) International Soft law. *The Journal of Legal Analysis*. 2(1). P. 178.

Holt, M. and Andrews, A. (2014) Nuclear Power Plant Security and Vulnerabilities. P11. Available from: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1486_web.pdf [Accessed 10 May 2015].

Hathaway, O. A. et al. (2012) The Law of Cyber-Attack. *California Law Review* 100(4). P. 826.

Kesler, B. (2011) The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights* 10(1). P. 16-18. Available from http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI-v10-I1_Kesler.pdf [Accessed 15 May 2015]

Mrabit, K. (2014) IAEA Office of Nuclear Security's Initiatives in Cyber and Information Security. [Online] IAEA, PowerPoint Presentation. Available from: https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf [Accessed 14 May 2015]

Shackelford, J. S. (2014) *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. New York: Cambridge University Press.

Stoiber, C. et al. (2003) *Handbook on Nuclear Law*. Vienna: IAEA. P.4.

IAEA (2011) International Legal Framework for Nuclear Security. IAEA International Law Series No.4. Available from: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1486_web.pdf [Accessed 2 June 2015].

ADDRESSING THE SECURITY-DEVELOPMENT NEXUS IN CONFLICT-AFFECTED COUNTRIES: POST-2015 PERSPECTIVES AND WAY FORWARD

Rossella Marangio
PhD Candidate in International Relations
Politics, Human Rights and Sustainability Programme
Sant'Anna School of Advanced Studies
r.marangio@sssup.it

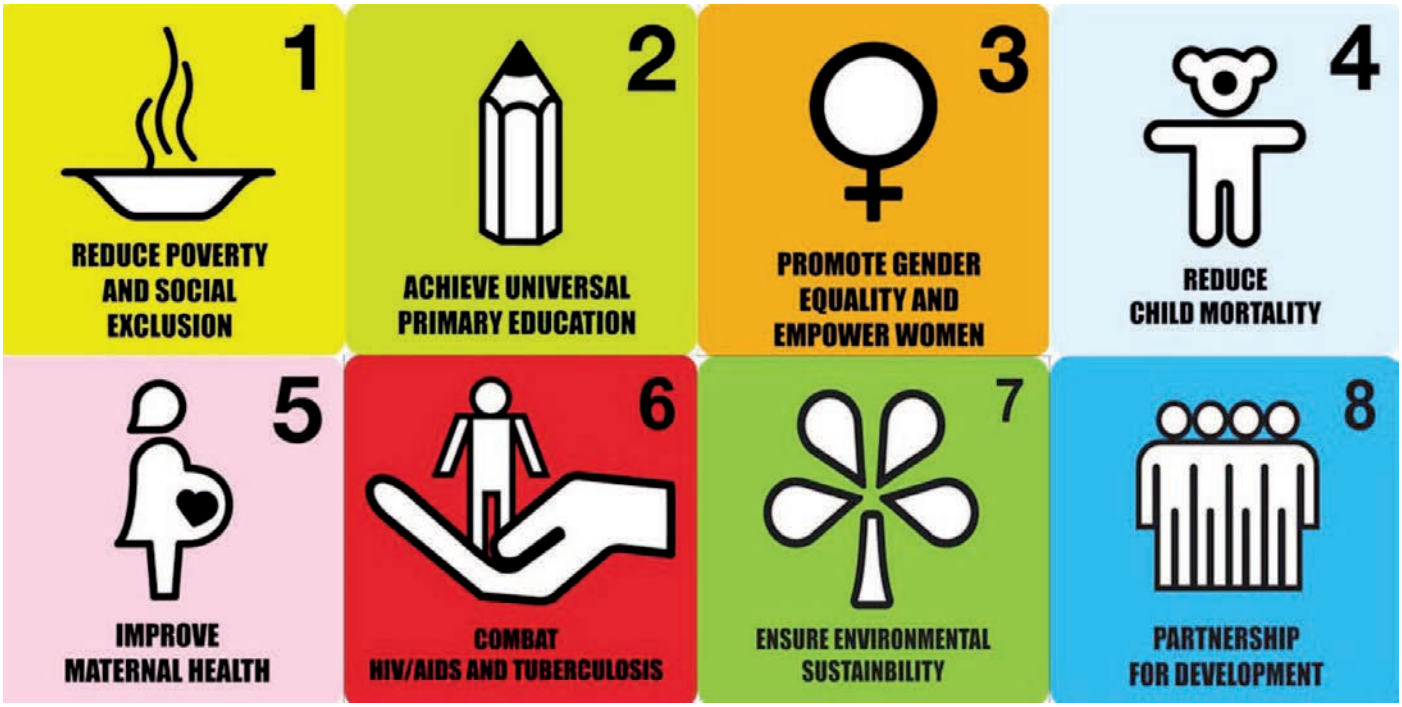
Abstract

In conflict-affected countries, security and development are particularly intertwined policies. The security-development nexus has been widely inserted into policy planning to tackle root causes of conflict and, as the Millenium Development Goals (MDGs) expire this year, the policy challenge on how to address security and development concerns at the same time re-acquires vigour. The paper analyses the shortcomings of a narrow conceptualisation and implementation of the security-development nexus and it argues that a multi-dimensional bottom-up approach best fits the purpose of addressing the root causes of conflict by intervening on the nexus.

Keywords

Security; development; security-development nexus; post-2015 agenda; resilience.

The Millenium Development Goals (http://www.un.org/millenniumgoals/)



Introduction

Conflict-affected countries present a particularly challenging environment for the international community because of the impact that conflict has on both international security and individuals. Moreover, the spillover effect on neighbouring countries that has occurred in many areas of the world has drawn the attention on the need to tackle violent conflict at an early stage, if not to prevent conflict from breaking into violence, and to address its root causes.

In this context, the 'security-development nexus' concept has been formulated and further developed both in policy documents and in academic research in order to express the interrelation between security and development, which had previously been dealt with separately. The need for this conceptualisation had emerged progressively after empirical findings pointed out a relation, or at least the widespread co-existence, of underdevelopment and conflict (Hurwitz & Peake 2004). Nowadays, poverty and violence have been identified as being intertwined (Ikejiaku 2012, 127; Denney 2013, 3). There is, however, little evidence and little agreement on the nature of their relation and the magnitude of mutual influence, namely whether it is poverty that prevents violence from stopping or security that constitutes a pre-requisite for development or how they are interconnected. In this respect, the debate seems to be highly influenced by what authors consider as the most pressing issue between the two policies. Thus, a dichotomy has emerged between those who place security as a pre-condition of development and those who supports the idea that development policies should be treated as independent to avoid a 'securitisation' of development (Chandler 2007, 362-363; Denney 2013, 2-3).

This paper is not going to analyse these competing views on the security-development nexus, on the contrary it is going to adopt an all-encompassing viewpoint in which development and security are understood as complementary policies that may generate positive outputs if jointly addressed (UN General Assembly Resolution 2005). Starting from the premise that decreased poverty rates and violence are strictly intertwined[1], this paper investigates the challenges of addressing the security-development nexus in the international actions towards conflict-affected countries and its potential for breaking the poverty-conflict cycle.

In the first section, an analysis of the international actions undertaken so far in addressing the security-development nexus in conflict-affected countries is provided with the aim to identify major shortcomings linked with the conceptualisation and the implementation of security-development related policies. Secondly, the paper presents and analyses the potential of conceptualising and implementing a multi-dimensional approach to the security-development nexus, which consists in linking the local, regional and international levels. Thirdly, a brief scrutiny of the risks and opportunities offered by a complex system of governance is presented. Finally, the paper will draw some conclusions and provide some recommendations on how to best address these challenges.

[1] Ikejiaku (2012) offers a summary of the literature on the topic.

The security-development nexus: a unidimensional, inward-looking record

The security-development nexus represents a highly complex policy and theoretical challenge due to its multidimensional character and the amount of involved actors and fora. As the period of application of the Millenium Development Goals (MDGs)[2] will expire at the end of 2015, the debate on whether and how security concerns should be channelled through development policies is witnessing a revival with regard to both policy formulation and implementation. In fact, security and its broader links to development had been mostly neglected in the formulation of the MDGs in 2000, while the emphasis was put on the individual dimension of security to be promoted through targets that mostly developed and upgraded the concept of human security[3].

However, at the end of the period of implementation of the MDGs, evidence shows that conflict-affected countries have been left behind in the pursuit of this concept of human security (UN System Task Team on the Post-2015 UN Development Agenda 2012,18; Denney 2013, 2), thus calling for revised action to tackle the persistent problems related to these scenarios. Thus, the issue of how to address the security-development nexus is far from being solved in policy-making; on the contrary, the record of the MDGs shows that the individual dimension does not suffice to effectively tackle the broader issue of security and development in conflict areas (UNDG Millennium Development Task Force 2013).

Despite the discourse about overcoming a state-centred approach to security launched with the MDGs, conceptualising the security-development nexus at a macro level seems to be necessary in order for these policies to be effective. The unidimensional character, attributed with the focus on human security, to the security-development nexus constitutes, in fact, one major shortcoming in its implementation, as tackling human security in a context of widespread conflict may be more than challenging.[4] The MDGs record indicates that a country-based approach should be included in the policies addressing the nexus and this stance has been supported by the consultations undertaken for the post-2015 development agenda.

Several reports presented at UN level and, in particular, the Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda presented in 2013 highlight the role of reliable and functioning institutions in positively influence both security and development (de Weijer & Knoll 2013, 3-4; High-Level Panel of Eminent Persons on the Post-2015 Development Agenda 2013, 9). However, since conflict-affected countries are generally struggling to build well-functioning institutions, the acknowledgement of their mediating role in mainstreaming security and development goals does not offer any concrete solution to the problem. Yet, it remains important to acknowledge the complexity and the interconnections between problems in order to avoid narrow-focused policies.

In this context, the New Deal initiative launched in 2011 by the International Dialogue on Peacebuilding and Statebuilding[5] constitutes an important governance instrument to specifically address the situation in conflict-affected countries. In fact, the New Deal offers a flexible platform for discussion between donors and recipients which places security and institution building at its core. Indeed, through setting a number of goals divided into three different pillars[6] and foreseeing the adoption of country-specific roadmaps, the New Deal initiative overcomes the unidimensional character of the policies launched with the MDGs and asserts the need for comprehensive and aggregate-level policies in addressing the security-development nexus. Also for this reason, it has been suggested to include the New Deal in the post-2015 development agenda, but the opposition of some countries such as Brazil – accusing the process of being donor-led – seems to push to abandon the idea (de Weijer & Knoll 2013, 5; Denney 2012, 12-14). However, the initiative points out some relevant features: first, it focuses on the peculiarities of conflict-affected countries, thus calling for targeted actions; secondly, it arguably empowers recipient initiatives that could contribute to modifying the donor-recipient relations; thirdly, it provides flexibility by encouraging country-specific policy planning.

Notwithstanding, one dimension can arguably be said to be missing: the regional dimension. Several conflicts worldwide – and in particular in Africa where most of the conflict-affected countries are – present an important regional dimension that implies both the potential for spillover and the role of neighbouring countries within the conflicts. Clear examples in this sense are, for instance, Somalia and the Democratic Republic of Congo (DRC), where persistent conflicts

[2] The MDGs are a set of eight time-bound targets adopted at the United Nations Millennium Declaration in 2000. For more information: http://www.un.org/millenniumgoals/.

[3] The concept of human security has been widely defined as concerning freedom from fear and freedom from want by the 1994 UNDP Human Development Report (Denney 2013, 2). In general, the individual dimension of security has to be interpreted as opposed to more traditional state-centred approaches to security (see Denney 2013, 2-3).

[4] No significant improvements have been recorded in conflict-affected countries in terms of MDG targets (de Weijer and Anna Knoll 2013, 2).

[5] The Dialogue was created in 2008 under the impulse of the 2005 Paris Declaration on aid effectiveness. Nowadays it brings together conflict-affected countries, international partners and civil society. In 2011, the New Deal for engagement in fragile states was launched in Busan at the 4th High Level Forum in 2011 in Busan. Further information may be found at the following links: http://www.pbsbdialogue.org/; http://www.newdeal4peace.org/.

[6] The three pillars are: the Peacebuilding and Statebuilding Goals (PSGs), FOCUS and TRUST. They are strictly related with the first one setting goals and the other two providing concrete steps and methods for implementation. For further information see: http://www.newdeal-4peace.org/new-deal-snapshot/.

cannot be explained only by taking into consideration domestic dynamics (Autesserre 2010; Guglielmo 2008). The same logics also apply to more recent conflicts emerged in the Sahel, Central Africa, Arabia peninsula, etc. Thus, effective conceptualisation and policy-making should also take into account the regional dimension in order to have an impact.

A few actors have started supporting this idea by adopting regional policies, like in the case of the European Union (EU) that adopted this approach both through its partnership with the African Union (AU) and the launch of the so-called regional strategies and the comprehensive approach[7]. However, these initiatives mainly address the institutional dimension of the security-development nexus, the focus being on streamlining institutions and policy procedures to implement whole-of-government approaches. In fact, the institutional dimension has been the core of international discussions on how to implement security and development policies. As said, although this is obviously an important side of security-development policies, it underestimates the interlocking role that dimensions such as the regional, national and individual have in addressing the security-development nexus effectively. In the end, the record of security-development nexus policies has been mostly unidimensional focusing almost exclusively on human security and inward looking by catalysing efforts on the institutional set-up rather than engaging with a more locally grounded assessment of needs and inclusive dialogues on action.

Reversing the approach: bottom-up processes to build resilience, institutions and peace

The current discussion on the post-2015 development agenda tries to promote inclusive consultations with different stakeholders worldwide (Zupi 2013), thus recognising the importance of involving not only a diversified range of actors, but also multiple dimensions. At the end of the process, proposals shall be submitted to the inter-governmental approval at the UN General Assembly in September 2015 together with the reports addressed to the UN Secretary General. As far as the linkage between security and development is concerned, one crucial point under discussion is whether security-related concerns should be inserted as a separate target in the list of the new Sustainable Development Goals (SDGs)[8] or if they should form a horizontal issue, thus making all targets 'conflict-sensitive' (Denney 2012, 5-6).

Nevertheless, based on the previous reasoning on the nature and complexity of the security-development nexus, this debate seems to suffer from the same inward-looking stance on the issue. As the core problem is to determine how to address both the security-development nexus and the issue of good governance, it could be useful to revert the process by adopting a bottom-up approach that would enable to consider different layers, namely the local, regional and international levels, starting from the closest level possible to individuals and communities.

In fact, the current situation in the international scenario suggests that externally imposed institutions or democratisation paths do not necessarily take root; on the contrary, they mostly lead to further negative externalities – an example of which can be terrorism – that reiterate the conflict. When applied to conflict-affected societies, the concept of resilience also seems to indicate that a community-based approach may provide a better fit for investing in the security-development nexus (see also Chandler 2015).[9] In fact, even if the current debate on the post-2015 agenda is trying to include the macro-dimension to tackle the problems of conflict-affected societies, it may still lack a mediating layer between human- and state-security: the community level.

The relevance of community-based approaches has acquired attention in the past years in particular in the development field, but it has been significantly side-lined in security-oriented policies. The latter, in fact, have been mainly focusing on the state level as the appropriate dimension to tackle broad security issues. The human security approach has challenged this assumption, but it has not provided an effective conceptualisation for policies and their implementation. On the one hand, human security has been mainly addressed through development policies and, on the other hand, as already discussed, it has adopted a narrow focus on security that does not help in exiting the loop of poverty and conflict faced by many conflict-affected countries. The additional community dimension could provide an apt level for addressing core issues of the 'security-development dilemma' such as which policy should intervene first and which policy deserves greatest attention and at which phase of the intervention. A community-based approach could provide the missing link between human- and state-security. Furthermore, it could also function as a catalyst for shifting from violent conflict to reconciliation

[7] The EU has launched three 'regional strategies' for the Horn of Africa, the Sahel and the Great Lakes regions and it has subsequently launched an overarching Comprehensive Approach framework with the Commission and High Representative Joint Communication to the European Parliament and the Council 'The EU's comprehensive approach to external conflict and crises' in 2013. Further information may be found at: http://europa.eu/rapid/press-release_IP-13-1236_en.htm.

[8] SDGs should replace the MDGs as from 2016. For further information see: https://sustainabledevelopment.un.org/index.php?menu=1565.

[9] Resilience is defined as 'the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organizing itself to increase its capacity for learning from past disasters for better future protection and to improve risk reduction measures.' (UN/ISDR 2005).

dynamics, thus paving the way for both peace and the establishment of legitimate institutions.
Therefore, a more effective approach to the security-development nexus should combine all different dimensions in order to maximise its chances of having an impact. Only in this case one could qualify the approach as a truly comprehensive one.

Govern the complex: multi-layered governance in addressing the security-development nexus

The security-development nexus also presents a number of problems in terms of governance, in addition to the already quite complex framework of conceptualisation and policy-making. In fact, it combines multiple intersecting governance areas that further complicate its analysis and question the effectiveness of the related policies. Development and security policies surely constitute the two core governance areas to which the security-development nexus relates, but others also intersect with the security-development nexus such as the environmental and climate change regimes in addition to the separate branch of governance areas directly addressing the nexus. Furthermore, each of these regimes[10] falls under the competence of a multitude of state-, intergovernmental and supranational actors such as the UN, the EU, the AU, the OECD, and more traditionally states. The interconnected nature of these regimes might indicate the emergence of a regime complex around the concept of security-development nexus[11]. Further research may investigate whether a regime complex has truly emerged by analysing more closely the interactions among diversified governance structures and regimes, but it is important to note that the complexity of 'multi-layered' governance around the concept of security-development nexus may represent both a window of opportunity and a challenge *per se* to policy planning and implementation. On the one hand, intensified discussions and multiple fora may provide the opportunity to streamline diversified policies – traditionally addressed as independent – into comprehensive frameworks for action by adopting, for instance, multi-dimensional planning or joint indicators to assess and address specific needs. On the other hand, complexity may also hinder effective planning and implementation, for instance, by creating competition among the regimes or the governance structures instead of synergies.
The above-mentioned risk is even greater if the supposed security-development nexus regimes continue to adopt unidimensional and inward-looking approaches. In fact, this kind of focus may amplify the importance of governance areas and structures at the detriment of the effectiveness of both policy planning and implementation. On the contrary, a multi-dimensional result-oriented approach presents the potential for reducing the risk of governance hindrances by shifting the focus on desired outcomes rather than procedures. In the same line, bottom-up approaches building on existent social structures rather than externally imposed paths would undermine the risk of self-interested behaviour on the side of donors or partner countries which sometimes may use security-development policies to foster their agendas rather than addressing the root causes of conflict or poverty.

Conclusion

The security-development nexus presents a number of highly challenging issues as regards both its conceptualisation and its channelling through policy planning and implementation. The paper assumed security and development as interconnected policies that can create positive synergies to exit the loop of poverty and conflict if combined.
An account of the record in addressing the security-development nexus has identified the focus on human security only and the emphasis on institutional developments as too narrow to positively impact conflict-affected countries. On the contrary, a multi-dimensional approach to the security-development nexus has been proposed as necessary to grasp the complexity of the problem and deliver effective policies. In the same light, the paper argues that a bottom-up approach is complementary to the classical top-down one, especially to favour the establishment of legitimate and reliable institutions. Moreover, a community-based approach has been put forward as the missing link between human- and state-security and the level that can best serve the purpose of security-development nexus policies. Finally, the paper has pointed out some considerations on the opportunities and risks that may derive from a highly complex set of regimes that find some interconnections at the juncture of the security-development nexus. Against this backdrop, result-oriented policy planning and implementation calibrated on local needs may limit the risks of both governance hindrance and actors' self-interested behaviour in acting within the security-development nexus.
The post-2015 development agenda has tried to overcome some of the shortcomings of the MDGs in addressing the security-development nexus, but further efforts in including flexible and targeted conceptualisation and implementation is necessary to break the vicious circle of poverty and conflict. A better understanding of the complexity of conflict-affected countries and the different layers that characterise contemporary conflicts is necessary in order to effectively

[10] A regime is here understood as an international regime as defined by Krasner (1982, 186): 'principles, norms, rules and decision-making procedures around which actor expectations converge in a given issue-area'.

[11] Raustiala and Victor (2004, 279) define a regime complex as 'an array of partial overlapping and non-hierarchical institutions governing a particular issue-area'.

intervene along the security-development nexus. Bottom-up and community-based approaches constitute to date the neglected dimensions of the problem and the aspects on which the international community should focus to improve its chances of having an impact on the ground.

References

Autesserre, S. (2010) *The Trouble with Congo: Local Violence and the Failure of International Peacebuilding*. Cambridge: Cambridge University Press.

Chandler, D. (2007) The security–development nexus and the rise of 'anti-foreign policy. *Journal of International Relations and Development*, 10 362–386.

Chandler, D., (2015). Rethinking the Conflict-Poverty Nexus: From Securitising Intervention to Resilience. *Stability: International Journal of Security and Development*. 4(1) Art. 13. Available from http://www.stabilityjournal.org/articles/10.5334/sta.fb/# [Accessed 30 May 2015].

De Weijer, F. and Knoll, A. (2013) Joining forces for peace post-2015. *ECDPM Briefing Note* 53. Available from http://ecdpm.org/publications/joining-forces-peace-post-2015/ [Accessed 29 May 2015].

Denney L. (2013) Consulting the evidence: How conflict and violence can best be included in the post-2015 development agenda. *Shaping policy for development ODI*. Available from http://www.odi.org/publications/7622-conflict-violence-post-2015 [Accessed 28 May 2015].

Denney, L. (2012) *Security: The missing bottom of the Millennium Development Goals? Prospects for inclusion in the post-MDG development framework*. London: ODI. Available from http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7788.pdf [Accessed 30 May 2015].

European Commission and High Representative for CFSP/CSDP (2013) *Joint Communication to the European Parliament and the Council: The EU's comprehensive approach to external conflict and crises*. JOIN(2013) 30 final. Brussels: European Commission. Available from http://www.eeas.europa.eu/statements/docs/2013/131211_03_en.pdf [Accessed 2 June 2015].

Guglielmo, M. (2008) *Somalia: Le ragioni storiche del conflitto*. Lungavilla: Edizioni Altravista.

High-Level Panel of Eminent Persons on the Post-2015 Development Agenda (2013) *A New Global Partnership: Eradicate Poverty and Transform Economies through Sustainable Development: the Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda*. Available from http://www.un.org/sg/management/hlppost2015.shtml [Accessed 30 May 2015].

Hurwitz, A. and Peake, G. (2004) Strengthening the Security-Development Nexus: Assessing International Policy and Practice Since the 1990s. *International Peace Academy Conference Report*. New York: IPA. Available from http://www.gsdrc.org/go/display&type=Document&id=4363 [Accessed 1 June 2015].

Ikejiaku, B-V. (2012) Poverty-Conflict Nexus: The Contentious Issue Revisited. *European Journal of Sustainable Development*, 1(2) 127-150.

Krasner, S. (1982) Structural causes and regime consequences: regimes as intervening variables. *International Organization*, 36(2) 185-205.

Raustiala, K. and Victor, D. (2004) The Regime Complex for Plant Genetic Resources. *International Organization*, 58 277-309.

Stern, M. and Öjendal, J. (2010) Mapping the Security-Development Nexus: Conflict, Complexity, Cacophony, Convergence? *Security Dialogue*, 41(1) 5-30.

UN General Assembly (2005) *Resolution on 2005 World Summit Outcome*. A/RES/60/1. New York: UN. Available from http://www.un.org/Docs/journal/asp/ws.asp?m=A/RES/60/1 [Accessed 29 May 2015].

UN Secretariat of the International Strategy for Disaster Reduction (2005) *Terminology: Basic terms of disaster risk reduction*. New York: UN/ISDR. Available from http://www.unisdr.org/2004/wcdr-dialogue/terminology.htm [Accessed 30 May 2015].

UN System Task Team on the Post-2015 UN Development Agenda (2012) *Realizing the Future We Want for All – Report to the Secretary-General*. New York: UN. Available from http://www.un.org/en/development/desa/policy/untaskteam_undf/report.shtml [Accessed 29 May 2015].

UNDG Millennium Development Task Force (2013) *A Million Voices: The World We Want – A Sustainable Future with Dignity for All*. New York: UN. Available from https://www.worldwewant2015.org/file/388792/view/422422 [Accessed 30 May 2015].

UNDP (1994) *New Dimensions of Human Security – Human Development Report*. New York: UNDP. Available from http://hdr.undp.org/en/reports/global/hdr1994/chapters/ [Accessed 2 June 2015].

Zupi, M. (2013) L'Agenda di sviluppo post 2015. *Osservatorio di Politica Internazionale: Approfondimenti*, 79. Roma: CeSPI.

REHABILITATING THE INDOCTRINATED

Priya Sara Mathews,
PhD Candidate Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
priyasmathews@gmail.com

Abstract

One of the major challenges that the world is facing today is the growing threat of ISIS. This terrorist organisation has grown at an astonishing rate and, disturbingly, has managed to recruit many young educated Europeans or Europe based youth. The paper attempts to touch upon the question of what can be done about these youngsters, who to some extent demonstrate the failure of our society today, if they are ever captured and brought back. Simply detaining them indefinitely in prison or meting out some other harsher punishment seems to ignore the real issue and furthermore appears to turn a blind eye on what is troubling these young people. The paper would like to explore the possibility of implementing one of the methods of justice used in post-civil war nations, specifically Restorative Justice, to entertain the possibility that these youngsters could, one day, become productive members of the society.

Keywords

Radicalisation, ISIS, rehabilitation, restorative justice, European youth, European Union, de-radicalisation.

Introduction

Over the past years reports about the Islamic State of Iraq and Syria (ISIS) and its growing influence both in Syria and Iraq has been an almost daily occurrence. Declaring itself as Islamic State and growing at an alarming rate, ISIS seems to be yet another among an increasing number of Islamic Terrorists groups in the region, the most well known of which in recent times was Al-Qaeda. The vitriolic rhetoric of its members and its uncompromisingly violent nature have made it a significant threat to most modern countries. Moreover, several foreigners have travelled to the region to join the "State". Some estimates show that around 20,000 foreigners in general, 4,000 Europeans in particular, have left their countries to be part of ISIS. The United Kingdom (UK) in fact appears to have provided the highest number of foreign fighters from Europe, with an estimated 500-600 people who have joined ISIS (Saltman and Dow 2015).

These figures show quite clearly that radicalisation of European citizens and the rising extremism in Europe are pressing issues that need to be urgently addressed. Research has shown that most of the terrorist offences of the past decade have been committed by those under the age of 30. Moreover, the process of radicalisation appears to take hold in youth as young as 16 (House of Commons Home Affairs Committee 2012). The issue that the current situation puts forth is twofold:
1) What can be done to prevent radicalisation and extremism;
2) How to manage those terrorists who have been captured or who return back to their home countries. There are several interesting researches that deal with radicalisation and its prevention; however, this paper will attempt to propose a plausible option for the second part of the problem.

The proposed question might seem banal or naive as incarceration for life and/or harsher penalties might seem to some as the most obvious ways to deal with terrorists. However, these have been the methods used until now and it does not appear to have made the situation any better. As a matter of fact, the amount of terrorist activity seems to be rising; in 2012 to 2013 alone, there was a 61 % increase in the number of deaths due to terrorist activities (Institute of Economics & Peace 2014). Furthermore, taking into consideration that several of these terrorists started their process of radicalisation when they were still minors, one cannot help but wonder if a better approach could have been taken into consideration in order to counter this problem. This is not a completely unfathomable option. Denmark, in fact, has already paved the way for this by offering rehabilitation rather than criminal retribution to those returning back from ISIS (Hooper 2014; Sengupta 2014).

In post-conflict civil war situations, in an attempt to rebuild a ravaged place, often restorative justice has been used. It is a way of enabling the victim to move forward and the offender to make amends for the grief caused and to take responsibility for their actions. This paper will look at how these post-conflict justice methods along with steps for de-radicalisation can be used to rehabilitate those young terrorists who return to their home country.

ISIS: Background and History

Although to many it may appear as though ISIS became powerful almost overnight, the rise of the terrorist organisation has been over a decade in the making. It went through various transformations and name changes before evolving into its current form. Some traces its origins to "Jama'at-al tawhid wa'al-Jihad", set up in 2002 by a Jordian Abu Musat al Zarqawi. In 2004, after having plead allegiance to Osama-bin-Laden, the organisation changed its name to "Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn", although it was

most commonly referred to as Al-Qaeeda in Iraq (AQI). Several other organisations joined AQI until it became the umbrella organizsation "Mujahideen Shura Council" (MSC) (UCDP Conflict Encyclopedia 2006). In 2010, Abu Bakr Al Baghdadi became its leader. Three years later, in April 2013 he announced the merging of forces in Iraq and Syria and the formation of the Islamic State in Iraq and the Levant (ISIL) more commonly known as ISIS (BBC News 2014).

ISIS aims to be a caliphate, with Baghdadi as its caliph, and it believes that all Muslims in the world must swear allegiance to it. An area of around 40,000 sq km to 90,000 sq km is said to be under its control, with territories including Mosul, Tikrit, Falluia, Tal Afar (Iraq) and Raqq (Syria). It is considered to be the richest jihadist organisation in the world with around $ 2 billion and there is believed to be around 8 million people living under its control (BBC News 2014; BBC News 2014).

Expansion and Recruitment

A significant number of ISIS fighters belong neither to Iraq nor to Syria and this has occurred mainly thanks to their efficient use of the Internet. For an organisation that seems to eschew all modern instruments, ISIS appears to have a very prominent presence in the virtual world. Many fighters have put uploaded *youtube* videos, they are active on social networks such as *Twitter*, *Facebook*, *Instagram* and *Tumblr* and it is through these channels that they are able to recruit new members. Technology has helped them reach a larger audience to an extent that was impossible to other organisations[1] (BBC News 2014; Hoyle, Bradford and Frennett 2015; Khaleeli 2014).

[1] There has also been a significant number of young teenage girls who have made their way to Syria after having met these recruiters on-line. It has been estimated that around 550 of the foreigners immigrating to Syria are women. (BBC News, 2014; Khaleeli, 2014).

The profile of a terrorist, however, is not that one can easily draw. Interestingly, even within Europe the profile of those who are allegedly joining ISIS seem to vary from country to country. The English recruits appear to be good students, well liked by their peers and far from the image of the social outcast. This can be seen both in the case of 'Jihadi John', the Kuwait-born UK based, ISIS fighter or in any of the three English teenage girls who made their way from London to Syria (Casciani 2015; De Freytas-Tammura 2015; BBC News 2015). One of the reasons for this phenomenon can be found in the fact that many of the universities in the UK have Islamic groups where sometimes extremist preachers are given a platform to speak. In France, where the Muslim population accounts for 7-10% of the total population but around half of its prison population (Khosrokhavar 2015), the situation appears to be a little different. According to Farhad Khosrokhava, French Islamic terrorists have a typical path:
'*alienation from the dominant culture, thanks partly to joblessness and discrimination in blighted neighborhoods; a turn to petty crime, which leads to prison, and then more crime and more prison; religious awakening and radicalization; and an initiatory journey to a Muslim country like Syria, Afghanistan or Yemen to train for jihad*' (Khosrokhavar 2015).

In both cases the vulnerability of those recruited is quite clear to see: where on the one hand there are young enquiring minds who are given the skewed view of world events, on the other hand there are those who feel like they are always on the outside looking in. The growing Islamophobia in Europe and the western world in general is used by many of the recruiters to convince the youth that they need to stand up and prevent the persecution of their religion and religious fellow men (Benali 2015; Nawaz 2015).

Radicalisation: a brief overview

In spite of the fact that religious ideology tends to play a significant role in luring young European Muslims to join ISIS, the process of radicalisation whether that of a Islamist or a neo-Nazi follows basically the same trajectory. Advocates who at one time worked with neo-Nazis feel that, like Nazism, Islamic extremism among the young is more connected to young people's susceptibility to the ideology (de Pommereau 2015). Ultimately, according to Mücke, Head of Violence Prevention Network (VPN) in Berlin:
'*They are both fascist ideologies. One is using a certain idea of the nation, the other is using religion as its instrument.*' (de Pommereau 2015)

Those at risk of being radicalised are usually youth who have had their self-esteem eroded and are searching for a sense of identity. They find themselves drawn to this narrative which gives them a purpose and makes them part of a greater goal; thus, giving them a sense of belonging and a way to act based on their resentment (Benali 2015; Benhold 2015; Mooney 2014).

Moreover, recruiters tend to play on young people's sense of victimisation, social injustice, their idealism and commitment to their religion. They are made to view the use of violence as the only means of achieving their goals. Furthermore, they stop viewing their adversary as human and thus releasing themselves from the responsibility of the atrocities they commit (Wessells 2005).

Restorative Justice

The criminal justice system as we know it, values objectivity and consistency in its attempt to provide justice. In addition, it works more on the principle of retribution. Restorative justice instead works on the idea that as crime hurts, justice should heal. This provides the victims with closure and the ability to move on and

rebuild their lives and at the same time it gives the offenders a chance to face up to their responsibility and realise the repercussions of their actions. According to Marty Price, '*Instead of viewing crime as a violation of law, restorative justice emphasizes one fundamental fact: crime damages people, communities and relationships.*' In this sense restorative justice is a way through which relationships can be restored (Marty Price 2001; Braithwaite 2004; Llewellyn 2006).

Restorative justice is forward looking since it aims not to dwell on the horrors of the past, but rather to focus on building relationships among individuals and the community and to create a future that is more just (Llewellyn 2006). Thus, for restorative justice it is crucial that during the process the focus is on healing rather than punishing; healing the victim and undoing the hurt and healing the offenders by rebuilding his or her moral and social selves and thus healing the community at large (Michael Wenzel 2008).

There are various forms of restorative justice, the most common of which are the Victim-Offender Mediation (VOM) and the victim-offender reconciliation program (VORP). These offer the opportunity for the victim and perpetrator to be face to face in the presence of a mediator, thus humanising the victims who have been previously de-humanised by the offender. In addition, these programs make the offenders take responsibility for their actions. Moreover forgiveness, which is often emphasised in many post-conflict situations, especially after a civil war, can also be addressed during the process of VOM (Marty Price 2001).

Reintegration is by no means an easy feat. According to René Girard, '*Once aroused, the urge to violence triggers certain physical changes that prepare men's bodies for battle. This set toward violence lingers on'* (Girard 1977); thus, reintegration into society will not be an easy process for these extremists and would require extensive psycho-social support. As this has already been done for child soldiers who undergo rehabilitation and reintegration, a similar process could be drawn for these fighters as well (Wessells 2005). Rehabilitation can only work if it allows for the assumption that radical individuals can be convinced to stop their association with terrorist organisations and to relinquish their commitment to them (Mullins 2010).

Conclusion

It is understandably difficult to imagine that the people who are depicted in the news and shown in *youtube* videos beheading and massacring people can be rehabilitated and reintegrated into the society. However, there are many European youth who go to Syria imaging that they are standing up for the oppressed or fighting against a tyrant, without completely understanding what exactly they are getting themselves into (Hooper 2014). Among them, there are those who, just like child soldiers, were brought in when they were too young and therefore they are not able to understand the implications of their actions.

In this day and age when human relationships and connections are becoming more and more disjointed and where young people have more virtual friends than real ones, trying to rebuild relationships would be more beneficial than incarceration, not only for the individual, but also for the community as a whole. Moreover, places like Guantanamo are exactly what the recruiters point to get more young people convinced that they were right all along. However, if the option of rehabilitation together with reintegration is possible there could be, eventually, a place for those who are disillusioned by what they see when they reach Syria and want to come back home. It would also encourage those who are still staying back for the fear of being imprisoned immediately to consider the error of their ways.

Finally, it is worth pointing out that this paper does not really focus on Islam or Muslims, despite referring to the terrorists as Islamist terrorists. One of the major reasons for this is that, as it was discovered during the research carried out for this paper, most of the youngsters who are radicalised do not have a very firm background in religion. It has been noted by many that those captured seem to be novices as far as the religion is concerned (Washington Blog 2014). They do not speak or read Arabic and they are usually exposed to the Quran by means of other extremists. They have been referred to as such here only as it is the commonly used term at the moment.

This paper aims only to provide an alternative option: further and more in-depth research might help show whether this process would be feasible and successful or not. Nevertheless, talking about justice in terms of punishment seems rather oxymoronic and counter productive; and as of now, it has not really proved to be otherwise.

References

BBC News (2014) A Point of View: Isis and what it means to be modern. *BBC News*, Available from http://www.bbc.com/news/magazine-28246732 [Accessed 10 April 2015].

BBC News (2015) Missing teenagers have crossed into Syria, Met Police say. *BBC News*, Available from http://www.bbc.com/news/uk-31612666 [Accessed 15 April 2015].

BBC News (2014) What is Islamic State?. *BBC News*, Available from http://www.bbc.com/news/world-middle-east-29052144 [Accessed 10 April 2015].

Benali, A. (2015) From Teenage Angst to Jihad. The Anger of Europe, Äôs Young Marginalized Muslims. *The New York Times,* Available from http://www.nytimes.com/2015/01/14/opinion/the-anger-of-europes-young-marginalized-muslims.html [Accessed 1 May 2015].

Benhold, K. (2015) Same Anger, Different Ideologies: Radical Muslim and Neo-Nazi. *The New York Times,* Available from http://www.nytimes.com/2015/03/06/world/europe/two-outcomes-similar-paths-radical-muslim-and-neo-nazi.html [Accessed 1 May 2015].

Braithwaite, J. (2004) Restorative Justice and De-Professionalization. *The Good Society* 13(1), pp. 28-31.

Casciani, D. (2015) Islamic State: Profile of Mohammed Emwazi aka 'Jihadi John'. *BBC News*, Available from http://www.bbc.com/news/uk-31641569 [Accessed 20 April 2015].

De Freytas-Tamura, K. (2015), Teenage Girl Leaves for ISIS, and Others Follow. *The New York Times,* Available from http://www.nytimes.com/2015/02/25/world/from-studious-teenager-to-isis-recruiter.html?partner=socialflow&tsmid=tw-nytimes&_r=0 [Accessed 20 April 2015].

De Pommereau, I. (2015) To fight homegrown jihadis, Germany takes lesson from battle with neo-Nazis, Available from http://www.csmonitor.com/World/Europe/2015/0226/To-fight-homegrown-jihadis-Germany-takes-lesson-from-battle-with-neo-Nazis [Accessed 27 June 2015].

Girard, R. (1977) *Violence and the sacred*. Baltimore: Johns Hopkins University Press.

Hooper, S. (2014) Denmark introduces rehab for Syrian fighters, Available from http://www.aljazeera.com/indepth/features/2014/09/denmark-introduces-rehab-syrian-fighters-201496125229948625.html [Accessed 15 April 2015].

House of Commons Home Affairs Committee (2012) Roots of violent radicalisation. Available from http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144602.htm (Accessed 2 July 2015).

Hoyle, C., Bradford, A. and Frenett, R. (2015) *Becoming Mulan? Female Western Migrants to ISIS*. Institute for Strategic Dialogue.

Institute for Economics & Peace (2014) *Global Terrorism Index: Measuring and Understanding the Impact of Terrorism,* Institute for Economics & Peace, Available from http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf (Accessed 2 July 2015).

Khaleeli, H. (2014) The British women married to jihad. *The Guardian,* Available from http://www.theguardian.com/world/2014/sep/06/british-women-married-to-jihad-isis-syria [Accessed 27 April 2015].

Khosrokhavar, F. (2015) The Mill of Muslim Radicalism in France. *The New York Times*, Available from http://www.nytimes.com/2015/01/26/opinion/the-mill-of-muslim-radicalism-in-france.html?_r=0 [Accessed 2 July 2015].

Llewellyn, J. (2006) Restorative Justice in Transitions and Beyond. In: Borer, T. ed. *The Truth: Truth Telling and Peace Building in Post-Conflict Societies*. 1st ed. Notre Dame, Indiana: University of Notre Dame Press, 83-113.

Mooney, C. (2014) Here are the psychological reasons why an American might join ISIS, Available from http://www.motherjones.com/politics/2014/08/inquiring-minds-arie-kruglanski-psychology-extremism-isis [Accessed 29 April 2015].

Mullins, S. (2010), Rehabilitation of Islamist terrorists: Lessons from criminology. *Dynamics of Asymmetric Conflict* 3(3), 162-193.

Nawaz, M. (2015), The Education of Jihadi John, *The New York Times,* Available from http://www.nytimes.com/2015/03/03/opinion/the-education-of-jihadi-john.html?_r=0 [Accessed 28 April 2015].

Price, M. (2015), VORP - Articles: Personalizing Crime? Available from http://www.vorp.com/articles/justice.html [Accessed 30 April 2015].

Saltman, E. and Dow, M. (2015), Islamic State: How foreigners are helped to reach Syria and Iraq. *BBC News*, Available from http://www.bbc.com/news/uk-31607728 [Accessed: 9 April 2015].

Sengupta, K. 2014. Denmark offers rehabilitation - not punishment - to returning jihadis. *The Independent*. Available at: http://Denmark offers rehabilitation - not punishment - to returning jihadis [Accessed: 15 April 2015].

Ucdp.uu.se, (2015), Database - Uppsala Conflict Data Program (UCDP), Available from http://www.ucdp.uu.se/gpdatabase/gpcountry.php?id=77&regionSelect=10-Middle_East# [Accessed 20 April 2015].

Wenzel, M., Okimoto, T., Feather, N. and Platow, M. (2008) Retributive and restorative justice. *Law and Human Behavior* 32(5), 375-389, Available from http://dtserv2.compsy.uni-jena.de/ws2011/sozpsy_uj/52038358/content.nsf/Pages/4388366485FDC8F4C125792F0040662C/$FILE/Wenzel_2008_RetributiveAndRestorativeJustice.pdf [Accessed 28 April 2015].Wessells, M. (2005), Child Soldiers, Peace Education, and Postconflict Reconstruction for Peace. *Theory Into Practice* 44(4), 363-369.

ORGANISED CRIME AND INTERNATIONAL ORDER: NORMATIVE AND PRACTICAL CHALLENGES

Luca Raineri
PhD Candidate
Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
lu.raineri@sssup.it

Abstract

The emergence of transnational organised crime as an actor capable to affect international peace and security poses interesting challenges, both theoretically and practically, to the international system. Despite an increased attention to these phenomena, sheer numbers may be misleading and imply inappropriate responses, the most important of which are analysed in detail herein. The article suggests that a more fine-grained, qualitative reading of the social function performed by organised crime, especially in conflict-torn settings, will be key to addressing these challenges in a more coherent and appropriate manner.

Introduction

The rise of unconventional threats to international peace and security has brought a considerable amount of literature, both of academic and practitioner origin, to critically reconsider the adequacy of the mainstream approaches to IR. The present article focuses on the progressive emergence of (transnational) organised crime (T)OC as a political phenomenon whose relevance cannot be underestimated in many theatres where the international community is currently engaged, including peace-building and peace-keeping operations. A recent assessment argues that TOC is directly affecting 21 UN peace missions throughout the world, and in 12 cases organised crime is explicitly mentioned in the mission's mandate (Kemp et al. 2013). This evidence obliges to reconsider the structuralist assumptions of the neorealist thinking (Waltz 1979), according to which states, supposedly unitary and homogeneous, are the only relevant actors of the international arena, and therefore the only subjects, or objects, of internationally relevant threats. Similarly, this evidence questions the traditional division of labour of the international system, that would tend to confine organised crime within the boundaries of localized, minor disturbances to the internal order, with little impact in the international arena, and therefore better dealt-with by national law-enforcement apparatuses.

The present article aims to explore the main challenges that the international community faces when dealing with organised crime as a threat to international peace and security. The fact that (T)OC straddles across the borders of the internal and the international realms of policy and security concerns makes of transnational organised crime an object that is particularly hard to capture, let alone to handle. In first place, the progressive emergence of the phenomenon of organised crime to the attention of the international community will be retraced. Furthermore, the article proposes a critical review of the main approaches that have been conceptualized and tentatively implemented by the international community, especially in the framework of peace operations, in order to concretely come to terms, in the ground, with the challenges posed by (T)OC as a threat to international peace and security. The impacts and drawbacks of these approaches will be analysed, and linked to their implicit assumptions, both theoretical and normative. In conclusion, the article argues that transnational criminal actors and organised criminal networks should not be neglected when dealing with today's international peace and security concerns. Nevertheless, such a reframing of the international peace agenda brings in, together with new actors, also new theoretical puzzles and practical challenges that don't seem to have found, till today, a satisfactory solution. The present work aims to identify, clarify and conceptualize some of the emerging theoretical and practical problems that are before us, while suggesting some tentative solutions.

Disentangling organised crime as a peace spoiler

In recent years one finds no lack of studies, statements and official declarations put forward by an increasing amount of international bodies and agencies that call for an enhanced attention to (T)OC as an emerging, definite threat to international peace and security.

In 2004, organised crime entered for the first time the arena of the international policy concerns, as it was ranked among the top-10 global security priorities identified by the UN High Level Panel on Threats, Challenges and Change's report: *A More Secure World, Our Shared Responsibility* (UN 2004). Since then, OC is increasingly mentioned in the mandates of UN peacekeeping and peace-building operations[1]. In 2011, the World Bank's *World Development Report*, authoritatively called to acknowledge «the repetitive and interlinked nature of conflict, and the increasing challenge of organised crime» (World Bank 2011: 181). Overall, in the decade 2004 – 2014 (T)OC has been mentioned in 77 resolutions or presidential statements of the UN Security Council (Shaw et al. 2014).

The rationale behind such a dramatic increase of attention by the international community can be attributed to at least two sets of concerns: the changing nature of contemporary organised violence, expressed by the figures of conflicts' body-count; the estimation of the impressive amount of resources stockpiled and managed by organised criminal networks worldwide, whose potential conversion into military might has suddenly appeared more threatening than ever.

Albeit imprecisely, the number of yearly victims captures a significant indicator of the impact of organised crime, especially when compared to other suppliers of organised violence. In this sense, two major reports published in 2011 marked a turning point for the recognition of (T)OC as a major threat to international order. That year, according to a World Health Organization (WHO) report, violence in all its forms (including structural violence, see Galtung 1969) accounted for the loss of about 1,5 millions lives, out of which 486,000 were to be attributed to inter-personal violence (including crime), and just 86,000 to war or other forms of conflict (WHO 2013). These figures roughly correspond to the ones put forward by Geneva Declaration on Armed Violence and Development's *Global burden of armed violence* 2011 report. Further research into specific case studies reported that in places like Guatemala, more than 15 years after the formal end of the civil war, «clandestine armed groups with deep ties to organised crime fuel Guatemala's sky-high homicide rate (c.39 per 100,000 people) – a rate similar to that during the most fatal years of the recent US occupation of Iraq» (Cockayne 2013: 6).

Albeit impressive, however, these figures can be misleading and deserve some critical circumspection. Beyond the sheer number of direct fatalities, indirect or structural violence (including famines, non-access to health facilities, loss of incomes etc.) strike hard the survivors, let alone the displaced, injured, orphans or handicapped persons, for many years beyond the formal end of hostilities. The indirect consequences of conflicts are deemed to be responsible of four times as many deaths as the number of fatalities captured by the body count (Geneva Declaration 2011). Consequently, one may argue that the reported above discrepancy between conflict-related and crime-related victims might be attributed not just – somehow fatalistically – to the changing

[1] In 2005 the UN Secretary-General's Special Envoy to Kosovo recognized that «organized crime and corruption have been characterized as the biggest threats to the stability of Kosovo and to the sustainability of its institutions», UN Security Council, Annex: *A Comprehensive Review of the Situation in Kosovo*, UN Doc. S/2005/635, October 7, 2005, p. 13.

"nature" of contemporary violence, but to a combination of successful peace theories and practices – addressing the most conventional forms of inter-state violence – and equally disastrous records of post-war practices of peacebuilding and statebuilding. Had conventional inter-state conflicts to make a comeback, the figures would probably be very different. A renewed attention to (T)OC as a relevant threat to international peace and security should therefore complement, and not simply replace, the existing tools for international conflict prevention and mitigation at the disposal to the international community.

The increased attention to TOC as a threat to international peace and security is also probably due to the concerns raised by the unprecedented amount of economic resources that are reportedly amassed by organised criminal networks worldwide. The estimated GDP of some non-state criminal actors outweighs the one of some sovereign States: according to a recent survey (Kemp et al. 2013), the opium racket is said to earn the Taliban some 125 millions dollars per year; in DRC the value of gold illegally mined and smuggled reaches 1,2 billion dollars per year; the protection racket is supposed to earn the Somali Shabaab about 80 millions dollars per year, and in Iraq, even before the Islamic State arose, about 200.000 oil barrels per day were illegally siphoned by local (T)OC networks and injected into black markets. Were this wealth converted into military resources, the standard argument goes (somehow simplistically), criminal actors would probably give a hard time to many conventional state-sponsored standing armies. And from this perspective, it would be pointless to linger in the neorealist assumption that TOC is by definition unable to affect international order. Such argument somehow parallels the one produced by political geographers in the early 1990s (Agnew and Corbridge 1995), where states were ranked according to their GDPs alongside with transnational corporations, in order to show the magnitude and significance of private actors in the emerging global economy.

Today, however, it seems clear that the argument of the state's capture by the external 'aggression' of exogenous non-state actors, whether legal or criminal economic entrepreneurs, lacks of convincing evidence. Critical border scholars, such as Sassen (2006) and

Mezzandra and Neilson (2012) have made abundantly clear that, in the framework of a globalized economy exposed to an internationalized environment, states have actively contributed to the demise of many of their own prerogatives in favour of non-state actors. The idea of a dichotomous cleavage and a competitive race between the public and the private, the political and the economic, the national and the international, is largely misleading, and should be reviewed in favour of a more nuanced articulation that nestles, rather than opposing, these dimensions. Just as much as this has been proven for the increasing role of transnational corporations in the global governance, a similar argument can arguably be made for the increasing relevance of organised crime for the international order. Indeed, the neorealist view implicitly assuming a radical opposition between the state and criminal organizations has been convincingly disputed, for instance, by Snyder and Duran-Martinez (2009), who stressed the importance of state-sponsored protection rackets. They argued that violence is reduced when OC enjoys some sort of 'legal' protection by state agencies that decide to turn a blind eye or to selectively enforce law provision in order to share the benefit of the criminal economy. The incestuous intimacy that often links, rather than opposing, states, law-enforcement apparatuses, and TOC, has been recognized by a growing number of scholars (Bayart 2004, Naim 2012, Kemp et al. 2013). In this sense, one can arguably agree with those analysts who recently emphasized that «even where no expressed desire for state capture or formal political power exists – and where, to the contrary, parasitic subsistence with the existing status quo and/or overtly apolitical and nonpartisan behaviour is a fundamental part of a group's survival strategy – it is useful to consider organised criminal groups' activity as essentially strategic, or political, with a small 'p'» (Banfield 2014: 22).

Three approaches to deal with organised crime in peace operations

Many different approaches have been attempted in order to deal with the challenges posed to the international order by the phenomena related to organised crime. Without pretending to conduct a systematic survey of all of them, we sketch herein the ones that have been most widely adopted, in order to highlight their respective merits and drawbacks.

1) Law-and-Order

This approach is eminently exemplified by the international war on drugs declared by the Nixon administration in the 1970s. The law-and-order policy simply aims at eradicating (T)OC, that is framed as a mere problem of public order, a simple deviance from a socially accepted norm that state-sponsored prohibition regimes (Andreas and Nadelmann 2006) are supposed to enforce. There is no lack of evidence, however, that contends that in particularly fragile contexts, and especially in post-conflict theatres, a purely repressive stance vis-à-vis criminal(ised) businesses risks to leave thousands of individuals

unemployed, who relied on the few opportunities offered by illegal economies for their survival. Contrarily to the stated aims, the attempted eradication of coca leaves and opium plantations in Colombia and Afghanistan respectively has ended up to reinforce criminal organizations that offered reliable protection to local producers. More often than not, an uncontrollable escalation of violence is likely to follow, which, while affecting civilians in first place, critically undermines the legitimacy of international interventions (OECD 2012).

The law-and-order approach to OC is thus often combined with counterinsurgency tactics. However, the blurring of law-enforcement ends pursued with military means can easily turn into a sterile and never-ending exercise of self-fuelling violence that might prove successful in short-ended military terms, but inconclusive and politically unsustainable in the long run (Porch 2013). It has been suggested that the politicization of every-day criminality and the criminalization of political enemies is largely ineffective on the ground, but it suitably serves the purpose to «accredit the ideological construction justifying the exorbitant strengthening of police powers and other law enforcement agencies» (Bayart 2004: 103).

2) Mediation.

Drawing on the consistent failures of law-and-order policies, it has been recently suggested that the traditional diplomatic tools of mediation can be relevant and applicable for states to deal with organised criminal actors (Cockayne 2013). According their proponents, «rather than peace operations being tasked to fight OC per se, they would be given the more limited, achievable, and measurable objective of managing organised criminality's impact on peace processes. The goal shifts from the endless fight against OC to the more immediate and reachable goal of managing organised crime» (Cockayne and Pfister 2008). Inspired by risk-reduction policies, an analogous view has been recently endorsed by an increasing number of regional organizations, such as the Latin American Initiative on Drugs and Democracy, and the West African Commission on Drugs (see OECD 2012), which emphasized the importance of managing the consequences of (T)OC instead of pretending to remove its root-causes.

However, it is hard to imagine what could possibly be a relevant common ground to sustain a meaningful mediation between state actors and non-state criminal(ised) organizations. 'Crime' is by definition a political label, rather than a phenomenological observation capturing some natural feature, and it is meant precisely to deny any political status to those it qualifies. 'Criminals' are no longer such as soon as they are recognized as potential interlocutors and involved in political negotiations. In some circumstance, such as in Salvador, the Catholic Church has been considered by both parties, the state and the criminal cartels, neutral and righteous enough to provide for a mediation. This option is however less realistic in secular, less cohesive, societies, or in places where the religious identity represents one of the conflictual issues at stake, like in Mali or in Afghanistan.

3) Stick and Carrot

This approach represents an attempt to win the hearts and minds of the target people susceptible to be seduced by the attractiveness of organised crime. This policy aims at combating organised crime through a more sophisticated combination of incentives (carrots) and disincentives (sticks). Instead of focusing uniquely on the supply side of crime, it also tries to address – and contain – the demand side.

The practical implementation of this approach remains however largely unsatisfactory. Based on the – often unquestioned – assumption that it is a profit-seeking orientation that drives the criminal conduct, incentives are often conceived in terms of material or economic gains entrusted to those who accept to drop every resort to violence for a progressive reintegration into the legality. Even if one leaves aside the obvious moral dilemmas of this approach, that seems to economically reward those who committed crimes, its sustainability remains questionable: often states – and namely fragile states where (T)OC is more prevalent (OECD 2012, Banfield 2014) – are incapable to match the resources that criminal networks can mobilize. International aid might temporarily address this imbalance, but in the long run it simply risks to further feed a bottom-less black hole of widespread corruption, especially where the oversight power of the donor country is particularly constrained.

Sanctions are often evoked on the disincentive side. It should be noticed, however, that sanctions represent one of the greatest opportunities for black markets to nestle and thrive (Andreas 2009); and «in extreme cases, the circumvention of sanctions may become associated with discourses of resistance to external pressure and other forms of belligerent rhetoric, as occurred in Iraq and Serbia in the 1990s» (Cockayne and Pfister 2008).

Conclusion: legitimacy, a normative challenge

Albeit in different ways, the existing policies aim at restructuring the full authority of the state, as well as law, order, compliance with social norms and monopoly of violence in areas where these are *de facto* disputed. Beyond the factual constraints, the existing literature and practice seem to have neglected to thoroughly examine the above-mentioned approaches from the normative point of view. We argue, however, that issues of legitimacy, even more than legality, are crucial in this domain.

As it was correctly observed: «international interventions that enforce international criminal norms that lack local legitimacy risk alienating local communities, exacerbating conflict» (Cockayne and Pfister 2008). Indeed, in contexts where formal state-sponsored service deliveries are underperforming or corrupted, organised criminal networks can easily be perceived as the providers of much-needed protection to powerless people and their businesses (Banfield 2014), as it proved to be the case in Latin America. In north Mali cross-border smuggling of any sorts has been existing for centuries, and its legitimacy, let alone its duration, far exceeds the one enjoyed by state's institution (Scheele 2012) reportedly affected by heavy corruption and discriminating practices. Under these circumstances, the labels of 'normal' and 'criminal' seem to reflect nothing but an arbitrary and foreign preference, if not a mere power relation.

In view of the considerable capital of social legitimacy that organised criminal actors still enjoy in many contexts, it seems urgent to foster a critical reflection about the normative assumptions that lay behind the framing of transnational organised crime as a threat to international peace and security.

References

Agnew J., Corbridge S. (1995), *Mastering Space*, Routledge, London.

Andreas P. (2009), "Symbiosis Between Peace Operations and Illicit Business in Bosnia", *International Peacekeeping*, 16(1), January 2009, pp.33-46.

Andreas P., Nadelmann E. (2006), *Policing the Globe. Criminalization and Crime Control in International Relations*, Oxford University Press, Oxford.

Banfield J. (2014), *Crime and Conflict, the New Challenge for Peacebuilding*, International Alert, London, July 2014.

Bayart J-F (2004), "Le crime transnational et la formation de l'Etat", *Politique Africaine*, 93, March 2004.

Cockayne J. (2013), "Strengthening mediation to deal with criminal agendas", *Oslo Forum Paper* n.2, Centre for Humanitarian Dialogue.

Cockayne J., Pfister D. (2008), "Peace Operations and Organised Crime", *Geneva Paper / IPI*, Geneva Center for Security Policy, Geneva.

Galtung J. (1969), "Violence, peace and peace research", *Journal of Peace Research* 6(3): 167–191.

Geneva Declaration (2011), *Global burden of armed violence 2011: Lethal encounters*, Geneva Declaration Secretariat, Geneva.

Kemp W., Shaw M., Boutellis A. (2013), *The elephant in the Room: how can peace operations deal with organized crime?*, IPI, June 2013.

Madsen F. (2009), *Transnational Organised Crime*, Routledge, London.

Naim M. (2012), "Mafia States, Organized Crime Takes Office", *Foreign Affairs*, May/June 2012.

OECD (2012), *Transnational Organised Crime and Fragile States*, (eds. Miraglia P., Ochoa F., Briscoe I.), OCDE Working Paper 5/2012, October 2012, Paris.

Porch D. (2013), *Counterinsurgency, Exposing the Myths of the new way of war*, Cambridge University Press, Cambridge.

Scheele J. (2012), *Smugglers and Saints of the Sahara: Regional Connectivity in the Twentieth Century*, Cambridge UP, Cambridge.

Shaw M., Reitano T., Hunter M. (2014), *Comprehensive assessment of Drug Trafficking and Organized Crime in West and Central Africa*, Report to the African Union, January 2014.

Snyder R., Duran-Martinez A. (2009), "Does illegality breed violence? Drug trafficking and state-sponsored protection rackets", *Crime Law and Social Change*, n. 52, pp. 253–273.

UN 2004, *A More Secure World, Our Shared Responsibility*, report to the Secretary General of the High Level Panel on Threats, Challenges and Change, New York

Waltz K. (1979), Theory of International Politics, Addison-Wesley Publisher, New York.

WHO (2013), *Global health estimates summary tables: Deaths by cause, age and sex*.

World Bank (2011), *World Development Report 2011: Conflict, Security, and Development*, World Bank, Washington, DC.

RESILIENCE, A NEW COUNTER-TERRORISM MEASURE: THE CASES OF THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION

Gergana Tzvetkova
PhD Candidate in International Relations
Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
g.tzvetkova@sssup.it

Abstract

This article discusses the importance of fear for terrorist activities and the significance of resilience as a counter-measure. We examine how the concept of resilience is reflected in recent official documents produced by the United States of America (USA) and the European Union (EU). The paper presents an assessment of recent concrete measures, adopted in the USA and the EU, which are likely to contribute to the strengthening of social resilience.

Keywords

Counter-terrorism, resilience, Unites States of America (USA), European Union (EU), fear management

1. Introduction

'America does not give in to fear.'
(President Barack Obama 2015)
'Europe will not give up its values.'
(High Representative/Vice-President Federica Mogherini 2015)

Terrorism tries to hide committed atrocities behind idealistic principles like self-determination, freedom, independence. Individuals and groups that engage in terrorism claim they are acting towards the achievement of a long-coveted goal of political, social or economic significance. Terrorists want people to believe they are sending a vital and appealing message. However, the only messages they communicate are the dangers of terror and the importance of finding a legitimate and sustainable reaction. Yet, the agility and adaptability of terrorist groups in the last decades and the societal backlash through stigmatisation of vulnerable groups have demonstrated the susceptibility of entire communities. The negative impact of terrorism can be described as twofold: first, it has made people more wary of their physical exposure and second, it has the potential of insidiously rearranging entire sets of individual and social values. In both directions, the impact is reinforced by terrorism's primary tool – fear. We, as people and citizens, are afraid of acts of violence and this affects our ability to respond to its threat. Fear creates a sense of tension in the community – a tension, which a democratic government is obliged to deal with. Thus, the governments of the United States of America (USA) and the Member States of the European Union (EU)[1] are responsible to face the challenges posed by terrorism and reduce the fear infused in their societies.

One of the possible responses in the wake of a terrorist act is retaliation through force. Our intention here is not to discuss arguments for and against the use of force as a reaction to aggression. Suffice it to say that a primary goal of the state is to protect its citizens, although the means used have been changing, due to the appearance of new threats or the rise of international organizations.[2] We argue that social crises caused by terrorist threats can also be dealt by strengthening the resilience of a community, by teaching it how to uphold values and practices targeted by terrorism. Societal resilience and fear management strategies have now entered the vocabulary of politicians and scholars that are trying to devise counter-terrorism methods. The first purpose of the present article is to discuss the importance of fear for terrorist ideologies and the significance of resilience as a counter-measure. Second, the paper will discuss how the concept of resilience is present in recent official documents and initiatives produced by the USA and the EU. Finally, it discusses concrete recent events in the the two polities that could contribute to the strengthening of social resilience.

This article argues that through creating fear, terrorism aims not only to destroy the physical integrity of the members of a society but also to shake the foundations of a society's value system. Therefore, counter-terrorism efforts should include elements of fear management and breed social resilience. Because it is the latter that might help a community preserve the alloy of distinctive features that makes it what it is. Resilience might be seen as acting in two directions. First, it is embodied in the ability to bounce back in the aftermath of a terrorist act. In this way, it is related to limiting the possibility of stigmatisation of certain groups. Second, resilience entails resistance to terrorist propaganda. This could be also seen as increasing the cohesion of the group and making it more inaccessible to terrorist groups from the inside.

2. Fear as a Tool

Prior to defining resilience and understanding its importance, we have to discuss the characteristics of fear as a major element of the terrorist toolbox. Zygmunt Bauman (2006, 2) defines fear as the 'name we give to our uncertainty: to our ignorance of the threat and of what is to be done'. Those succumbing to terrorism and those falling prey to fear are 'locked into a sort of liquid modern version of the *dance macabre*',

as they feed off each other's positive or negative emotions (Bauman 2006, 122). Globalization facilitated the spread of fear of terrorism. Globalized communication networks make us more informed but also increase the channels through which fear reaches us. The Islamic State (IS) uses on a daily basis social media to publish videos of its atrocious deeds. This has raised a new, important question for the journalistic profession – should media publish the videos to inform the people of the threat and the reach of ISIS or should it not because of values like decency and as an attempt to resist the terrorist groups by refusing to broadcast their message. No matter what individual journalists will answer, we can no longer isolate ourselves from terror even when spared from direct terrorist attacks. It has entered our TV, newsfeeds, social networks and ultimately our homes, rekindling our everyday fear of terrorism.

In his seminal work *A Philosophy of Fear*, Lars Svendsen (2008, 109) reminds us of the argument of some of his fellow philosophers about the possibility to regard fear as a 'resource for the community', which has a 'cohesive effect'. Further, in relation to the *War on terror*, he rightly notes that the fear brought by terrorism should not be combatted with the state-sponsored creation of even greater fear through the curtailment of civil liberties and rights – on the contrary, the fight against it should involve measures that uphold the values we are afraid for (Svendsen 2009, 122-123). Nevertheless, there is another equally dangerous social consequence of fear – 'hyper-emotional overreactions which may ultimately undermine social

[1] In this text, *American* will be used interchangeably with *US* and *European* will be used interchangeably with *EU*.

[2] International organizations not only restrain states in terms of the actions they are allowed to take; they also provide them with a broader forum where they could shape and discuss their interests.

and political unity', stigmatisation of certain groups, which in turn maximises the risk of radicalisation among these groups (Bakker and Veldhuis 2012, 4-5). Stigmatisation and radicalisation are valid problems today, often developing against the background of frantic media covering of specific events and populist outbursts.

3. The Concept of Resilience

Observations about the negative effects of fear and the need to overcome them, has made scholars and practitioners consider fear management and resilience-building when devising counter-terrorism policies. Resilience has been defined 'as a protective factor that limits the negative impact of terrorism on individuals and on society' (Bakker and Veldhuis 2012, 5). On a more abstract level, resilience is a state of mind that can fight the despair, hopelessness and demoralisation that terrorism brings (Waxman 2011). And it is exactly the desolation and disheartenment societies feel in the face of terrorism that rip them off of their values like strive towards freedom, transparency, non-discrimination and respect for human rights. It is then extremely important to foster resilience as a way of defending these values – in fact resilience is turning into a value itself, because it could hopefully become a distinctive characteristic of a healthy society that can both prevent terrorist attacks and recover quickly from them, should these occur. The mass vigils and marches that took place in Europe after the Charlie Hebdo attack that culminated in the world-famous slogan *Je Suis Charlie* might be considered a positive example. This slogan is now a cornerstone of the fight against terrorism and, above all, a very intimate expression of compassion and empathy. It essentially embodies personal identification with someone or something that has fallen prey to terrorism. The demonstration of compassion and strength through identification with the victims can be seen as an element of the shield against fear that resilience provides.

On a more practical level, public education and communication have been suggested as important tools for strengthening resilience. The International Centre for Counter-Terrorism (ICCT) suggests that: the public needs to be kept not only informed but also properly trained; communication with all relevant authorities and stakeholders should be maintained efficiently; there should be efforts to channel and mitigate the emotional answers to terrorist threat and acts (Bakker and Veldhuis 2012, 5-7). Along this line, experts from the ICCT define fear management as 'the efforts, undertaken by government institutions, prior, during and after situations of emergency and recovery, relating to a terrorist threat or attack, to manipulate the human capital in society in order to improve the positive, collective coping mechanisms of that society' (Bakker and De Graaf 2014, 1). It is undeniable that events like the burning of the Jordanian pilot by ISIS, the attacks against Charlie Hebdo in Paris or 9/ 11 are extremely traumatic – and not only for those directly affected. Unfortunately, resilience is not an inherent feature of human beings and societies. Instead, we are often afraid, uneasy and undecided, which sometimes makes us hide and turn our eyes away. But resilience can be taught, nurtured and encouraged.

In that relation, an important point, raised by Bakker and de Graaf (2014, 11), has to be mentioned – while resilience should be sought, this cannot be done by resorting to overly alarmist messages – instead, the mobilisation of the population should be done cautiously. For example, in the aftermath of a terrorist attack or in times of great social sensibility to terrorist-related issues, it is better to use toned-down language that does not fuel radicalisation and stigmatisation. The reason is that in the wake of a terrorist act, both society and government are more exposed to hate speech or radical actions, because they had become vulnerable and the normality of their everyday functioning has been disturbed. Acts of violence against certain social groups could eventually bring around their alienation, thus closing the vicious circle of fear, hatred, revenge seeking and intolerance that paves the way to new acts of terror.

Before discussing specific resilience-directed initiatives in the EU and the US, two clarifications are needed. First, the choice of exactly these two actors has been motivated by the increased exposure of the European and American public to terrorist acts since 9/11. This does not mean that other parts of the world do not suffer equally or even more from terrorism – just as one example, the Boko Haram barbarities in Nigeria prove otherwise. At the same time the US and the European countries have been in the avant-garde of terrorism and counter-terrorism research.[3] Second, prior to examining best practices, we should ponder on a twofold meaning of resilience. Examination of scholarly and policy-related literature demonstrates that on the one hand, we have resilience to terrorism as resistance to 'dark' emotions like scapegoating, stigmatisation and irrational panic among the population. On the other hand, resilience is the resistance to radicalisation among vulnerable groups themselves. These two notions of resilience are not in contradiction with each other – rather, they are complementary.

4. Resilience in the US Practice

Two of the Core Principles identified by the 2011 US National Strategy for Counterterrorism (2011) are very important for the focus of this article: Adherence to US Core Values and Building a Culture of Resilience. As to the first, the document points out that the loyalty to certain values has a twofold purpose: preserving the fabric of society and finding similarly-minded allies in the fight against terrorism. The mentioned Culture of Resilience is paid a special attention in another presidential document, the Presidential Policy Directive (PPD-8), which defines resilience as 'the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies' (USA. Homeland Security 2011). The presidential decree establishes the National Preparedness System to be devised and supervised by the Secretary of Homeland Security, who is supposed to issue regular National Preparedness Reports. The last[4] published report is of interest because it accounts for the

[3] The research centers in Washington DC, St. Andrews, Scotland and London are among the key research centers on terrorism and counter-terrorism studies in the world. BAKKER, E. (2013) Key authors and Centres. [Lecture notes] *Terrorism and Counterterrorism: Comparing Theory and Practice.* Leiden University. [Online] Available from https://www.coursera.org/learn/terrorism/lecture/P1Sk1/key-authors-centres [Accessed 12 May, 2005].

[4] As of 1 May, 2015.

Boston Marathon Bombing from April 2013.[5] Here are three findings of the 2014 Report that according to its authors demonstrate the better preparedness and resilience in the aftermath of the terrorist act (USA. Homeland Security 2014):

· Authorities made good use of established partnerships and platforms for sharing of information;
· 'Unprecedented information sharing' took place between investigators, the private sector and the public – the first regularly updated the other two groups how they can be of help, which resulted in many tips, videos and photos.
· One result of preliminary plans and exercises in Boston was the full mobilisation of hospitals in the area 'within moments of the second blast'.

The positive assessment of the reaction in the wake of the bombing goes beyond the accounts of official authorities. A report coming from an academic setting also concluded that '…Boston showed strength, resilience, even defiance – and these were key drivers of the overall outcomes … that is, of *Boston Strong*' (Leonard, Cole and Howitt 2014). The slogan and the movement *Boston Strong* are a powerful manifestation of the eagerness of the community to recover. The positive evaluation of the *Boston Strong* movement, from academics and practitioners alike, is a sign that it has the potential to turn into a best practice to be applied in the future in the US.

5. Resilience in the EU Practice

Unfortunately, Europe is not a stranger to terrorism too. The 2012 Burgas bus bombing reminded us how easy it is for a terrorist cell to move around united Europe and gain access to important transport hubs. After the 2015 terrorist attacks in several European cities, among which the one against *Charlie Hebdo* newspaper stands out, the danger of radicalisation has never been more acutely felt. Although counter-terrorism measures remain within the portfolio of Member States, several recent EU initiatives in the direction of resilience building deserve mentioning. The EU's Internal Security Fund is going to support projects that will contribute to 'Increased resilience among vulnerable individuals, communities and target groups' (European Commission. Directorate-General Home Affairs 2014). Establishing best practices and implementing well-devised initiatives will be especially important in the light of news about teenagers leaving European countries to join terrorist groups like the Islamic State. Probably the most popular cautionary tale for policymakers and practitioners of all kinds is the radicalisation of *Jihadi John* and the handling of his case by the relevant authorities (Engel and Kelly 2015). The Radicalisation Awareness Network (RAN), which falls under the 'PREVENT' strand of the EU Counter-Terrorism Strategy (Council of the European Union 2015) is collecting a database of best practices from Member States that aim at diminishing the possibility of radicalisation and enhancing resilience (European Commission. Migration and Home Affairs 2015).

6. By Way of Comparison

According to this brief, and by no means comprehensive, glance at EU and US findings and projects related to resilience, the use of the concept in the EU most often pertains to prevention of radicalisation within vulnerable groups. In the discussed US documents, the concept is more widely connected to the ability of the community to bounce back, to know how to react in the wake of terrorism. The reasons might be sought in the different standing of the two actors. The US is the declared primary enemy of many terrorist groups, while there are notable differences in this regard between European countries, i.e. some Member States are more threatened by terrorism than others. Second, as it was mentioned before, in the EU counter-terrorism strategies still belong mostly to national governments. Third, Europe is geographically closer to the areas where many terrorist groups operate. These three criteria may account for the difference in the understanding of resilience in the EU and the US. However, this difference does not mean the concept is devalued. On the contrary, in the future the transatlantic partners could only benefit from the differing approaches to resilience – resilience as community response and resilience as prevention of radicalisation – when devising efficient counter-terrorist strategies and policies. Resilience, thus, might be seen as an emerging value in itself encompassing social cohesion, solidarity and respect for deeply embedded social principles.

7. Conclusion

The purpose of this short article was to discuss resilience as an under-researched topic in counter-terrorism studies (Schmid 2011) and a new technique to apply in response to terrorist threats and acts. It is important to note that resilience is not simply resistance or opposition to terrorism, as these do not convey fully the psychological and emotional aspect of resilience. Without the communal cohesion and inner strength, resistance might lead to unwanted consequences. In counter-terrorism strategies resilience-building can be seen as the "missing link" between the much needed purely technical preparation of people for terrorist acts and the reliance on emotional coping mechanisms like marches, solidarity protests, etc. This is so because resilience presupposes not only readiness through education and training but also psychological alertness and strength to prevent both irrational distress and succumbing to destructive emotions.

[5] In April 2015, Dzhokhar Tsarnaev was found guilty on all 30 federal charges brought against him, one of which is the 'use of a weapon of mass destruction.' The *Boston Marathon Bombing* is considered a case of domestic terrorism. See: Goldman, 2015.

References

BAKKER, E. (2013) Key authors and Centres. [Lecture notes] *Terrorism and Counterterrorism: Comparing Theory and Practice.* Leiden University. [Online] Available from https://www.coursera.org/learn/terrorism/lecture/P1Sk1/key-authors-centres [Accessed 12 May 2005].

BAKKER, E. AND DE GRAAF. B. (2014) Towards a Theory of Fear Management in the Counterterrorism Domain: A Stocktaking approach. *ICCT Research Paper. International Centre for Counter-Terrorism – The Hague.* [Online] Jan. 2014 Available from - http://www.icct.nl/download/file/ICCT-Bakker-de-Graaf-Towards-A-Theory-of-Fear-Management-in-CT-January-2014.pdf [Accessed 20 February 2015].

BAKKER, E. AND VELDHUIS, T. (2012) A Fear Management Approach to Counter-Terrorism. *Discussion Paper. International Centre for Counter-Terrorism – The Hague.* [Online] Feb. 2012 Available from http://www.icct.nl/download/file/ICCT-Veldhuis-Bakker-Fear-Management-February-2012.pdf [Accessed 19 February 2015].

BAUMAN, Z. (2006) *Liquid Fear*, Cambridge: Polity Press.

ENGEL, P. AND KELLY, M.B. (2015) Questions surround British ISIS executioner Jihadi John's path to radicalization. *The Business Insider.* [online] 26 February 2015. Available from http://uk.businessinsider.com/british-isis-executioner-jihadi-johns-path-to-radicalization-2015-2?r=US [Accessed 1 May 2015].EUROPEAN COMMISSION. DIRECTORATE-GENERAL HOME AFFAIRS (2014). *INTERNAL SECURITY FUND POLICE (2014-2020) CALL FOR PROPOSALS – HOME/2014/ISFP/AG/RADX PREVENTING RADICALISATION TO TERRORISM AND VIOLENT EXTREMISM.* [Online] Available from http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/calls/2014/ispf-ag-radx/docs/isfp_2014_radx_call_en.pdf [Accessed 3 May 2015].

EUROPEAN COMMISSION. MIGRATION AND HOME AFFAIRS (2015) *RAN best practices collection.*[Online] Last update 2 April 2015. Available from http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-best-practices/index_en.htm [Accessed 3 May 2015].

EUROPEAN UNION DELEGATION TO THE UNITED NATIONS. (2015) S*peech by HRVP Mogherini at the Summit on Countering Violent Extremism*. [Online] Available from – http://eu-un.europa.eu/articles/en/article_16111_en.htm [Accessed 21 February 2015].

GOLDMAN, A. (2015) Tsarnaev found guilty on all counts in Boston Marathon bombing trial. *The Washington Post.* [Online] 8 April 2015. Available from http://www.washingtonpost.com/world/national-security/jury-weighs-verdict-for-second-day-in-boston-marathon-bombing-trial/2015/04/08/11755a56-ddf0-11e4-a500-1c5bb1d8ff6a_story.html [Accessed 1 May 2015].

LEONARD, H.B., COLE, C.M. AND HOWITT, A.M. (2014) Why Was Boston Strong? Lessons from the Boston Marathon Bombing. *Executive Summary. Harvard Kennedy School. Program on Crisis Leadership.* [Online] Available from http://www.hks.harvard.edu/content/download/67493/1242782/version/1/file/Summary_WhyWasBostonStrong.pdf [Accessed 3 May 2015].

SCHMID, A.D. (2011) 50 Un- and Under-researched Topics in the Field of (Counter-) Terrorism Studies. *Perspectives on Terrorism.* [Online] Vol 5, No 1 (2011) Available from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/schmid-under-researched-topics [Accessed 25 March 2015].

SVENDSEN, L. (2008) *A Philosophy of Fear,* London: Reaktion Books.

USA. HOMELAND SECURITY (2011). *Presidential Policy Directive / PPD-8: National Preparedness, 30 March 2011.* [Online] Available from http://www.dhs.gov/presidential-policy-directive-8-national-preparedness [Accessed 1 May 2015].

USA. HOMELAND SECURITY (2014). *National Preparedness Report*. [Online] 30 March 2014. Available from http://www.fema.gov/media-library-data/1409688068371-d71247cabc52a55de78305a4462d0e1a/2014%20NPR_FINAL_082914_508v11.pdf [Accessed 2 May 2015].

USA. THE WHITE HOUSE. OFFICE OF THE PRESS SECRETARY (2011). *Remarks by the President at "A Concert for Hope."* [Online] Available from https://www.whitehouse.gov/the-press-office/2011/09/11/remarks-president-concert-hope. [Accessed 15 April 2015].

USA. WHITE HOUSE (2011). *NATIONAL STRATEGY FOR COUNTERTERRORISM*. [Online] Available from https://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf [Accessed 20 February 2005].

WAXMAN, D. (2011) Living with terror, not Living in Terror: The Impact of Chronic Terrorism on Israeli Society. *Perspectives on Terrorism*. [Online] Vol 5, No 5-6 (2011) Available from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/living-with-terror/html [Accessed 25 March 2015].

CONTEMPORARY FOREIGN FIGHTERS: INTERPRETING THE THREAT AND ADDRESSING IT AT THE INTERNATIONAL LEVEL

Silvia Venier
PhD Candidate in International Law
Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
s.venier@sssup.it

Abstract

This paper aims at providing an overview of the Foreign Fighters (FFs) phenomenon in contemporary times, particularly in relation to the conflict in Syria. It explores the challenges in assessing the threats posed by FFs for Western States and in addressing them at the international level. It concludes by arguing for a more cautious approach while dealing with the complex challenges raised by contemporary FFs.

Keywords

Foreign Fighters, Terrorism, Security Council Resolution 2170 (2014), Security Council Resolution 2178 (2014), International Criminal Court.

Photo from http://vid.alarabiya.net/

1 Introduction

The phenomenon of Foreign Fighters (FFs), broadly defined as 'non-citizens of conflict states who join insurgencies during civil conflict' (Malet 2013, 9), is neither radically new nor uniquely Muslim. In the post-Westphalian era, there is a wide range of examples of armed volunteers joining a conflict in a foreign country, the Spanish Civil War being the most cited case in modern times. In the Muslim world, a turning point is represented by the so called 'Arab Afghans', volunteers from Arab countries who contributed to the local mujahedeen's *jihad* following the Soviet Union invasion of Afghanistan in 1979.
Especially after the Afghan war, FFs have been strongly associated with Jihadism or violent Islamism. Particularly since when FFs have been linked with the protracted civil war in Syria and the closely connected insurgency in Iraq, there is a growing tendency to conflate them with terrorism. Indeed, FFs are nowadays considered as a global issue, to be addressed with the adoption of specific measures at the international level. The major threat is currently posed by citizens of or residents in Western countries who join the conflict in Syria and can potentially return to their home countries in order to perpetrate terrorist attacks (the so-called 'blowback'). However, the risk posed by contemporary FFs remains a complex and still under-studied topic (Kraehemann 2014). Evidence on the subject is still limited, often classified or anecdotal. Few studies have analysed the process of FFs recruitment and mobilisation. There are contradictory views on FFs' actual role in the Syrian conflict, ranging from paramount contribution to fostering divisions and rivalries (Coticchia forthcoming). Moreover, the potential for blowback is still unclear, due to the lack of direct evidence and empirical data (Qureshi 2014).
According to Hegghammer (2010, 90) the Western tendency to conflate FFs with terrorism 'has been a major source of communication problems between the West and the Muslim world since the terrorist attacks of September 11, 2001', in particular consideration of the fact that the majority of the Muslim community differentiates between the two. This paper aims at discussing the reasons behind the new perception of FFs on contemporary times (section 2), and at exploring to what extent the conflation between FFs and terrorism is adequate to interpret such a complicate and dynamic phenomenon (section 3) as well as to address the challenges FFs pose at the international level (section 4). The conclusive remarks argue for a more cautious approach to be adopted while dealing with the complex challenges raised by contemporary FFs.

2. Foreign Fighters as a new terrorist threat

The interest of the international community in FFs has been growing significantly in the last few years. Two kinds of reasons may explain the new perception that FFs have acquired in contemporary times.
First, the new dimension mainly derives from the unprecedented number of FFs active in Syria. The latest estimates refer to an exponential growth of FFs, in particular between 2013 and 2014, turning Syria into 'the largest mobilisation of FFs in Muslim majority countries since 1945' (Neumann 2015). While the majority of FFs comes from Arab states[1], nearly a fifth is presumably composed of nationals of or residents in Western European countries[2]. In relation to the latter point, the potential return of FFs to the countries of origin with the intent to commit terroristic attacks is raising serious concerns in Western States. The increasingly widespread tendency to conflate FFs with terrorism is not only supported by the estimates that the al-Qaeda branch Al Nusra Front (ANF) and the Islamic State (IS) are attracting the vast majority of FFs, but also by the potential threat of 'blowback'. Second, the well-defined communication strategy adopted in particular by ANF and IS makes Syria (and the closely related conflict in Iraq) an interesting case study in relation to the new strategies, highly relying on social media, for FFs recruitment and mobilisation. It is not by chance that Syria has been defined as 'the most socially mediated conflict in history' (Lynch, Freelon and Aday 2014). By analysing the online open source material available on social media accounts of FFs of Western origin, a recent study found that Syria 'may, in fact, be the first conflict in which a large number of Western fighters have been documenting their experience of conflict in real-time'(Carter, Maher and Neumann 2014). Not only represent social media an essential source of information and inspiration for FFs, but the practice of sharing the atrocities committed through the internet has also profound implications on how the threat is perceived in the Western world.
These considerations may help in explaining the urgency to adopt measures at the international level aimed at addressing the risks posed by FFs to their countries of origin. The two Security Council Resolutions 2170 and 2178, adopted in 2014 under the United Nations Charter Chapter VII and formally linking FFs with terrorism by the introduction of the new terminology 'Foreign Terrorist Fighters' (FTFs), have been the most important measures taken at the international level. However, while addressing the FFs phenomenon,

[1] Especially Tunisia, Saudi Arabia, Morocco, Jordan.

[2] In particular France, Germany, United Kingdom, Belgium and Netherlands. Other Western countries involved in this phenomenon include Canada, United States, Australia and New Zealand (Neumann 2015).

policy makers are confronted with what Bakker, Paulussen and Entenmann (2014) describe as a 'three-fold challenge', comprising:

- risk-assessment related issues (i.e. finding a balance between under-estimating and over-emphasising the risks posed by FFs travelling and returning to Western countries);
- governance instruments (i.e. adopting consistent socio-political measures and comprehensive policies to deal with potential travellers and returning FFs);
- legal mechanisms available both at the international and domestic levels.

The following sections will focus in particular on the risk-assessment related issues and the legal measures adopted or currently under discussion at the international level. In section 3 the paper analyses the challenges in assessing the risks posed by contemporary FFs, focusing on how FFs can be categorised, what are the key motivations to join the conflict, what is the potential for returning home to carry out terrorist attacks. The most important measures adopted or under discussion at the international level aiming at dealing with FFs are briefly described in section 4, particularly focusing on Security Council (SC) Resolutions 2170 and 2178, and on the potential for a SC referral to the International Criminal Court.

3. Interpreting the threat

Due to the inadequacy of reliable data and the lack of empirical studies, a comprehensive interpretation of the contemporary FFs phenomenon and of the actual risks is not available. The main challenges relate to provide a coherent definition of the term, to interpret the main motivations behind FFs decision to join the conflict abroad as well as the different choices FFs can make after they took part in the conflict.

The difficulties related to categorising FFs as a specific group derive from the wide range of typologies of actors and of activities performed. FFs active in Syria are distinctive with respect to their background and motivations. They have joined not only IS and ANF, but also a wide range of other groups and fractions, including the Kurdish groups and the regular militias of the Damascus government (Neumann 2015). As per the activities they perform, these range from ideological or military training and fighting to perpetrating terrorist attacks or other serious crimes. The definitions of FFs currently available in the literature do not completely help in attributing a coherent focus to this phenomenon. Building upon Malet's definition, FFs have been more precisely identified as a category distinguished from mercenaries (whose motivation is usually financial rather than ideological or religious), from soldiers, returning diaspora members or exiled rebels, jihadists or international terrorists, who are usually specialised in violent extremism against non-combatants (Hegghammer 2010)[3]. More recent definitions suggest that the members of a diaspora or second-generation immigrants in Western countries should be included in the FFs category (Kraehemann 2014)[4], or that all foreign combatants who join one of the parties in the conflict, i.e. both state and non-state actors, should be considered as FFs (de Guttry, Capone, Paulussen forthcoming)[5].

Although overlaps and correlations between FFs and terrorists may emerge, blankly assuming that FFs are all terrorists may result in introducing concepts that are confusing. Indeed, there might be many differences between an individual who joins a conflict abroad with the primary intention to contribute to that conflict by fighting with local insurgents, and an actor who joins a terrorist organisation and receives military training with the intention to carry out a terrorist attack, either in the war zone or in the country of origin. Understanding what are the main motivations behind FFs' decision to join the conflict abroad is therefore another crucial element that has to be assessed. The narratives at the basis of FFs mobilisation have been categorised by Briggs and Frennet (2014) in humanitarian (aiming at opposing the brutality of a regime, e.g. the Assad regime), ideological (adhering to the ideology or the religious view of the group the FF has joined, e.g. IS or ANF), and identity-based motivations (driven by a search for identity and belonging). More research on the motivations behind FFs decisions would be important in order to understand what type of counter-narratives should be used and what type of efforts should be made to dissuade would-be volunteers to leave the country of origin.

In order to assess what is the actual threat FFs pose at the domestic level, the question also arises regarding the different choices made by FFs after having been involved in the Syrian conflict. The options available are many and difficult to assess. Based on an analysis of previous cases involving Western FFs, namely Afghanistan, Bosnia and Somalia, a recent study pointed out that the choice to return to a Western country and be involved in a terrorist activity is just one out of eight possible options after having fought abroad, while it remains unclear which options are more likely than others (de Roy van Zuijdewijn and Bakker 2014). In a research on variations in Western jihadists' choice between domestic and foreign fighting, Hegghammer (2013) points out that most Western FFs prefer to fight outside rather than at home, although the presence of FFs returnees increases the effectiveness of attacks in the West (the so-called 'veteran effect'). The author suggests three hypotheses to explain why foreign fighting is preferred to domestic fighting, namely opportunity (it is easier), training (it is more intense abroad) and norms (foreign fighting is viewed as more legitimate).

To conclude, an accurate risk-assessment in relation to contemporary Western FFs active in Syria implies conducting more research on their motivations to join the conflict, on the key factors driving their recruitment and mobilisation and on the choices they make afterwards. The risk of perpetrating a terrorist attack is only one of the multiple challenges Western FFs pose in case they return home; other (probably most pressing) issues may relate to the need to reintegrate them into society, by e.g. addressing war syndromes or post-traumatic stress disorders.

[3] According to Hegghammer, a FF is 'an agent who (1) has joined, and operates within the confines of an insurgency, (2) lacks the citizenship of the conflict state or kinship links to its warring factions, (3) lacks affiliations to an official military organisation, and (4) is unpaid'.

[4] This definition identifies a FF as 'an individual who leaves his or her country of origin or habitual residence to join a non-state armed group in an armed conflict abroad and who is primarily motivated by ideology, religion and/or kinship'.

[5] The definition reads 'Individuals, driven mainly by ideology, religion and/or kinship, who leave their country of origin or their country of habitual residence to join a party engaged in an armed conflict'.

4. Addressing the threat at the international level

Although the lack of response by the international community has been one of the salient features of the conflict in Syria since 2011, the exponential growth of Western FFs in this conflict has instead triggered a more concrete reaction at the international level. The phenomenon has turned into a global issue, deserving the attention of the international community, since the FFs-related concerns have been addressed by two Security Council (SC) Resolutions, S/RES/2170(2014) and S/RES/2178(2014), both adopted under the scope of the Chapter VII of the United Nations Charter. In addition, the potential for a SC referral to the International Criminal Court (ICC) is also being discussed in relation to the most serious crimes committed in Syria and Iraq.

In S/RES/2170(2014) FFs have been formally linked with terrorism through the introduction of the new terminology 'Foreign Terrorist Fighters' (FTFs). The Resolution states that the presence of FTFs in Syria and Iraq is 'exacerbating the conflict and contributing to violent radicalisation' and calls on Member States (MSs) to 'take measures to suppress the flow of foreign terrorist fighters' and 'to bring them to justice'. S/RES 2178(2014) specifically deals with FTFs, who are defined as 'individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict'. Although the inclusion of a specific definition is an innovative element and is important in order to deal more concretely with FFs (de Guttry forthcoming), concerns are still raised in relation to the potential for abuse by States in labelling individuals as FTFs, in consideration of the absence of, on one side, of an internationally-recognised definition of 'terrorism' and, on the other, of an ascertained legal definition of FFs. In addition, the SC Resolution definition seems particularly problematic in its final part when it refers to 'armed conflicts', considering the potential for contradictions between the international legal framework covering the prevention and suppression of terrorism and the International Humanitarian Law provisions applicable to non-international armed conflicts[6]. This resolution also calls on MSs 'to act cooperatively to prevent terrorist from exploiting technology, communications and resources to incite support for the terrorist acts'. The challenge here lies on the fact that measures adopted to limit the use of social media for FFs recruitment may imply imposing restrictions on the free flow of information and thus also on the possibility to make maximum use of information shared online by FFs for counter terrorism purposes.

A final consideration has to be made in relation to a possible referral to the ICC by the SC with regard to the most serious crimes that may have been committed in Syria (and Iraq) that may amount to war crimes, crimes against humanity and possibly genocide[7]. Since it is doubtful that Iraq and Syria, not Parties to the Rome Statute, will accept an *ad hoc jurisdiction*, a SC referral seems to be one of the two options available to hold IS members (including FFs) accountable for these crimes. Leaving aside the political considerations over the possibility for the resolution to be vetoed, a debate is growing within the academic community on whether the ICC could target only specific portions of the two states (e.g. the provinces controlled by IS), or even the specific groups (IS or ANF)[8]. The second option for the Court would be to intervene *proprio motu* (without a SC referral), by exercising personal jurisdiction over nationals of States parties to the Rome Statute, who have joined the conflict in Syria and Iraq and have been responsible for committing serious crimes. This seems to be particularly relevant with respect to crimes committed by FFs who are nationals of State Parties. However, in April 2015, the Chief Prosecutor admitted that this option is unlikely, considering that the perpetrators who are nationals of State parties do not seem to be among those 'most responsible'[9], and that the inquiry, if only based on nationality, would be highly fragmented and probably too selective, with the highest ranks of IS and ANF not being reached.

5. Conclusions

The FFs phenomenon is increasingly attracting much of the international community attention with particular reference to the recent developments in Syria and Iraq and the potential return of FFs to the countries of origin. The difficulties in obtaining reliable information and in providing coherent interpretations of such an intricate phenomenon seem to be at odds with the perceived need of urgency in adopting measures aimed at addressing the main risks it poses.

In this paper, the tendency to conflate contemporary FFs and international terrorism has been discussed from different perspectives, in particular related to risk-assessment issues and legal challenges at the international level. From this brief analysis, it can be grasped that an accurate risk-assessment in relation to contemporary Western FFs implies to conduct more research on their motivations to join the conflict, on the key factors driving their recruitment and mobilisation, and on the choices they make afterwards. There is also the need to research on the potential overlaps and contradictions of different legal provisions that may be applicable. In addition to the counter-terrorism framework, International Humanitarian Law and International Criminal Law may be of particular relevance. In particular, issues such as the potential overlap between FFs and terrorism, and the legal avenues to prevent FFs departure and their blowback, as well as to hold them accountable for the most serious crimes committed during the conflict abroad, seem particular relevant in this context.

The debate on FFs is still controversial, far from providing comprehensive answers to the many questions it poses. A more cautious approach to linking FFs and terrorism, that takes into account available evidence and aims at addressing the gaps and contradictions of the applicable international legal frameworks, seem to be the best at the disposal of the international community to deal with all these challenges.

6 For more details see Kraehenman 2014.

7 See the Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, 'Rule of Terror: Living under ISIS in Syria', 14th November 2014. Available from: http://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/HRC_CRP_ISIS_14Nov2014.pdf

8 See Skander Galand article on 'The Situation Concerning the Islamic State: Carte Blanche for the ICC if the Security Council Refers?', May 27th 2015, Available from: http://www.ejiltalk.org/the-situation-concerning-isis-carte-blanche-for-the-icc-if-the-security-council-refers/

9 See http://www.icc-cpi.int/en_menus/icc/press%20and%20media/press%20releases/Pages/otp-stat-08-04-2015-1.aspx.

References

Briggs, R., And Frennet, R. (2014) Foreign Fighters, The Challenge of Counter-Narratives. Institute fro Strategic Dialogue Report. Available from: http://www.strategicdialogue.org/Foreign_Fighters_paper_for_website_v0.6.pdf [Accessed 28 May 2015].

Carter, J. A., Maher, S., Neumann, P. R. (2014) #Greenbirds: Measuring importance and influence in Syrian Foreign Fighters Networks. ICSR Report. Available from: http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf [Accessed 28 May 2015].

De Guttry, A., Capone, F. And Paulussen, C. (eds.) (forthcoming) Foreign Fighters under International Law and beyond. Asser/Springer.

De Roy Van Zuijdewijn J. And Bakker E. (2014) Returning Western foreign fighters: The case of Afghanistan, Bosnia and Somalia. ICCT Background Note. Available from: http://www.icct.nl/download/file/ICCT-De-Roy-van-Zuijdewijn-Bakker-Returning-Western-Foreign-Fighters-June-2014.pdf [Accessed 28 May 2015]Hegghammer, T. (2010) The Rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad. *International Security*, Vol. 35, No. 3 (Winter 2010/11), pp. 53–94. Available from http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00023 [Accessed 28 May 2015].

Hegghammer, T. (2013) Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting, American Political Science Review, Vol. 107, Issue 01, February 2013, pp. 1-15. Available from http://hegghammer.com/_files/Hegghammer_-_Should_I_stay_or_should_I_go.pdf [Accessed 28 May 2015].

Kraehenmann, S., (2014) *Foreign Fighters under International Law*, Geneva Academy Of International Humanitarian Law And Human Rights Academy Briefing n°7, October 2014. Available from: http://www.geneva-academy.ch/docs/publications/Foreign%20Fighters_2015_WEB.pdf [Accessed 28 May 2015].

Lynch, M., Freelon, D., And Aday, S. (2014) Syria's socially mediated civil war. *Peaceworks* n°91. Available from : http://www.usip.org/sites/default/files/PW91-Syrias%20Socially%20Mediated%20Civil%20War.pdf [Accessed 28 May 2015].

Malet, D. (2013) Foreign Fighters: Transnational Identities in Foreign Conflicts. Oxford University Press.

Neumann, P. R. (2015) Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s. *International Centre for the Study of Radicalisation and Political Violence, ICSR Insight*. Available from: http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/ [Accessed 28 May 2015].

Qureshi, A. (2014) Blowback: Foreign Fighters and the threat they pose. CAGE Report. Available from: http://www.cageuk.org/sites/files/reports/A4_CAGE_SYRIA_REPORT.pdf [Accessed 28 May 2015].

CHALLENGES IN SEXUAL ORIENTATION AND GENDER IDENTITY-BASED ASYLUM CLAIMS: PROMOTING A WAY FORWARD TO THE PROTECTION OF LGBTI PEOPLE'S RIGHTS

Denise Venturi
PhD Candidate in International Law
Politics, Human Rights & Sustainability Programme
Sant'Anna School of Advanced Studies, Pisa, Italy
d.venturi@sssup.it

Abstract

The legal framework and the credibility assessment of LGBTI asylum claims raise several challenges, in particular within the European Union. The paper addresses these issues analysing the main problems posed by the 1951 Refugee Convention and the relevant European legislation. It proposes a forward-looking approach, in particular through the implementation of human rights law to the context of sexual orientation and gender identity-based asylum claims.

Keywords

LGBTI asylum seekers, sexual orientation, gender identity, particular social group, LGBTI human rights.

Introduction

The European Union (EU) is currently facing a dramatic increase in the number of people seeking sanctuary in one of its countries (UNHCR 2015). The fight against migrants' smugglers, the prevention of migrant deaths at sea and the respect of the obligation[1] to guarantee international protection to people who are eligible for it, are considered as top priorities that the EU has to deal with.

However, regarding the international obligations towards asylum seekers, light must be shed on another issue which is gaining increasing attention among practitioners and scholars: asylum claims based on sexual orientation and gender identity.[2] Claims presented by lesbian, gay, bisexual, transgender and intersex (LGBTI) people entail a wide range of implications from different points of view, such as the legal, the philosophical and the anthropological ones.

Although this topic is attracting more and more interest, exhaustive research has not been carried out yet, especially with regard to the EU (Jansen and Spijkerboer 2011, 13).[3] Moreover, at present there are no clear and well-established data available regarding the numbers of asylum applications filed in EU countries on the basis of sexual orientation and gender identity, because the vast majority of states do not collect specific statistics on the point. To date, the most comprehensive data available are those collected by the research "*Fleeing Homophobia*" (Jansen and Spijkerboer 2011). The report shows that only Belgium and Norway collect statistical data, while other EU countries present only approximate numbers (Jansen and Spijkerboer 2011, 15). This study has estimated that there are roughly "*up to 10.000 LGBTI related asylum applications in the European Union annually*" (Jansen and Spijkerboer 2011, 16). Notwithstanding, any analysis of figures on LGBTI asylum applicants should consider a higher number of cases than reports show. Hidden cases can be explained taking into account that applicants may be ashamed or reluctant to reveal the real reasons behind their claims, since they may be afraid of the impact that disclosure could have on their lives, such as repercussion in the family or in the reception facility (Jansen 2013, 17). Moreover, claimants may be unaware that they are entitled to protection against sexual orientation and gender identity-based persecution.

Fleeing persecution

Problems related to LGBTI asylum claims intertwine with the protection of LGBTI people's human rights. People who do not identify in the generally accepted notion of heterosexuality or in the traditional qualifications of socially constructed gender roles may suffer discrimination and even abuses. All over the world LGBTI people are exposed to human rights violations; abuses range from discrimination to hate speech, from denial to limitation of freedom, harassment, torture and killing (O'Flaherty and Fisher 2008, 208).

Mistreatments can be committed by community fellows or can be institutionalised by means of laws: currently, 76 countries criminalise same-sex relationships and at least 5 of them apply death penalty.[4] Directly or implicitly, state-sponsored homophobia (Carroll and Paoli Itaborahy 2015) has the effect to foster hatred and intolerance and to favour a culture of impunity, thus putting LGBTI people's lives at risk and further exacerbating tensions within the society. People who are exposed to acts of violence and who do not feel safe in their country of origins are forced to flee to another state, as it is the case for applicants who decide to seek sanctuary in the EU.

In the context of LGBTI asylum claims there are two issues of immediate importance: the application of the legal definition of 'refugee' to LGBTI asylum seekers and the problems related to the proof of such claims.

Challenges in the current legal framework

Even though sexual orientation and gender identity are not expressively included among the grounds of the Refugee Convention[5], persecution on those bases can constitute a valid reason for international protection.

Typically, LGBTI claims fall under the ground of 'membership of a particular social group' (UNHCR 2012, para 40), although some critical issues remain still open. Traditionally, the concept of 'social group' in the Refugee Convention envisages two alternative approaches: the '*protected characteristic*' and the '*social perception*' (UNHCR 2012, para 45).

The former refers to the group's immutable characteristic attached to the group as such. On the one hand, this approach underlines that the group deserves protection because of some innate specifications that are inherent to its members and, thus, linked to the concept of human dignity; hence, acts of persecutions carried out on the basis of such characteristics represent an attack to individuals' dignity and humanity. Therefore, sexual orientation and gender identity should be protected to the extent that a person should not be forced to change them or to conform to others' ideas or normative conceptions

[1] As commended by the 1951 United Nations Convention Relating to the Status of Refugees (Refugee Convention) and the relevant EU legislation on the point. The "Common European Asylum System" has its legal basis in Article 78 of the Treaty on the Functioning of the European Union and it is composed by the *Qualification Directive* (2011/95/EU), the *Procedure Directive* (2013/32/EU), the *Reception Conditions Directive* (2013/33/EU), the *Dublin III Regulation* (604/2013/EU) and the *EURODAC Regulation* (603/2013/EU).

[2] UNHCR (2012: 8) endorsed the definition of gender identity and sexual orientation given by the Preamble of the Yogyakarta Principles: "'*sexual orientation' to refer to each person's capacity for profound emotional, affectional and sexual attraction to, and intimate and sexual relations with, individuals of a different gender or the same gender or more than one gender; [...] 'gender identity' to refer to each person's deeply felt internal and individual experience of gender, which may or may not correspond with the sex assigned at birth, including the personal sense of the body (which may involve, if freely chosen, modification of bodily appearance or function by medical, surgical or other means) and other expressions of gender, including dress, speech and mannerisms*".

[3] Both from a quantitative and a qualitative point of view.

[4] These 5 countries are: Mauritania, Sudan, Iran, Saudi Arabia and Yemen. For more specific information see ILGA 2015.

5 Art. 1(a)(2) Refugee Convention: "*For the purpose of the present Convention, the term "refugee" shall apply to any person who: [...] 2. [...] owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it*".

Photo from: http://blog.amnestyusa.org

(UNHCR 2012, para 47). On the other hand, this interpretation risks to neglect that sexuality is not always fixed and immutable throughout a person's life (Cragnolini 2013, 100). Hence, if this aspect is not properly considered, it risks to deny cases that are instead worth of protection; for instance, a lesbian woman may not be considered as such because she has had children before.

The social perception approach, instead, focuses on whether the group shares some peculiar and common characteristics which makes it "*cognizable [...] from society at large*" (UNHCR 2012, para 45), thus emphasising the group's visibility within the society. Although this approach does not require the individual to have any feeling of common belonging or identification to a certain group (UNHCR 2012, para 48), it can be problematic for those asylum seekers who are obliged to conceal their identity in the country of origin. Moreover, it risks to reinforce stereotypes, since it leaves room for speculation on how LGBTI people should look or act. The UNHCR Guidelines on claims based on sexual orientation and/or gender identity point out that the group must be "*'cognizable' [...] in a more general, abstract sense*" within the society (UNHCR 2012, para 49); however, it is not very clear what this means in practical terms.

These concerns regarding the international legal framework couple with those posed by the EU legislation. Article 10 of the Qualification Directive 2011/95/EU explicitly mentions persecution based on sexual orientation and gender identity[6], thus acknowledging

[6] Article 10(1)(d) of the Qualification Directive: "*[...] Depending on the circumstances in the country of origin, a particular social group might include a group based on a common characteristic of sexual orientation.[...] Gender related aspects, including gender identity, shall be given due consideration for the purposes of determining membership of a particular social group or identifying a characteristic of such a group*".

its relevance among the range of elements to consider in judging on international protection. However, two points appear critical. Firstly, problems arise regarding the definition of '*particular social group*'. Differently from the Refugee Convention[7], the Qualification Directive requires the 'protected characteristic' and the 'social perception' approach to be present cumulatively.[8] Considering the unresolved issues connected to what exactly 'membership of a particular social group' entails, it seems that the formulation of Article 10(1)(d) further complicates and limits the decision of LGBTI claims.

Secondly, the Article further specifies that sexual orientation can be included among the characteristics of the social group '*depending on the circumstances in the country of origin*'. While this reference appears as a reminder to pay attention to the information available on the applicant's country of origin, at the same time it can lead to protection denials if not carefully applied. In fact, regarding the criminalisation of same-sex conducts, it has been argued that laws must not only be in place, but also enforced, so to have a 'well-founded fear of persecution'. Hence, considering the inclusion of sexual orientation as a group's characteristic depending on the circumstances in the country of origin may lead to think that in case of mere criminalisation, without enforcement, people are not entitled to international protection. However, this solution is not consistent with the protection of human rights and must be rejected. In fact, '*criminalisation reinforces a general climate of homophobia*' (Jansen 2013, 9). Moreover, it puts LGBTI people at risk at any time, since laws are still in place even if inactive; a change of government or in the judiciary system can easily lead to their actual application. In addition, this interpretation is inconsistent with Article 9(2)(b) of the Qualification Directive, which states that acts of persecution can originate from "*legal [...] measures which are in themselves discriminatory*"; thus, the existence of such provisions in itself amounts to persecution. Eventually, it clashes with the principle of non discrimination enshrined in Article 21[9] of the European Charter of Fundamental Rights (EU Charter) and also constitutes a serious limitation to the right to private life.

In conclusion, even though the inclusion of sexual orientation and gender identity in EU legislation shall be welcomed positively, concerns still remain regarding its consistency with the Refugee Convention and with the general protection of LGBTI people's rights; it seems that the formulation of the Qualification Directive restricts the possibilities for LGBTI asylum seekers. Furthermore, other aspects should be considered, namely those related to the reception of the Qualification Directive in the EU member states.

Credibility and burden of proof

In the context of asylum claims, credibility assessment is defined as "*the process of gathering relevant information from the applicant, examining it in the light of all the information available to the decision maker*" (UNHCR 2013, 27). While the issue of credibility lies at the core of all asylum claims, it acquires an additional meaning with regard to LGBTI applicants. Literature concurs in considering credibility as one of the most pressing issues to be addressed within this context, as well as one of the most under-researched (Jansen 2013, 15).

Addressing the problem related to credibility assessment requires to find a balance between states' need to investigate whether an application is sound and supported by adequate proofs vis-à-vis the individuals' need not to undergo intrusive and inappropriate procedures, in order to demonstrate that their application is motivated by persecution based on sexual orientation and/or gender identity. The main question is whether the person applying for international protection on such grounds is really (or is perceived as) a LGBTI individual (Middelkopp 2013, 156). This matter is closely related to the 'quantum of evidence' that is necessary to obtain the refugee status. At the moment there is no 'one-size-fits-all' solution to this problem and a common procedure has not been established yet at EU level, with the result that there is a '*huge diversity*' in the way LGBTI applications are assessed (Jansen 2013, 15). UNHCR reiterates the need for an '*individualized and sensitive*' assessment (UNHCR 2012, para 62); interviews should not revolve around the applicant's sexual practices, but should look to other elements, namely the personal narrative of shame, social stigma and self-identification.

It is also crucial the way in which results are interpreted. Stereotypes on LGBTI people's behaviour and appearance, as well as pre-constructed assumptions and cultural biases can result in the rejection of the application because the person does not correspond to the examiner's ideas of how a gay man or a lesbian woman should appear (Jansen 2013, 16). Thus, relying upon Western-constructed notions of sexuality and gender identity risks to overlook some fundamental elements.

Addressing protection gaps

As showed before, LGBTI asylum claims give raise to different kinds of problems, from several perspectives. Without being exhaustive, three main points can be taken into account to ensure better protection to LGBTI asylum seekers:

The evolving nature of international refugee law

The established legal framework provides the possibility for LGBTI people, owning a well-founded fear of persecution, to apply for international protection; however, it does not further clarify the aforementioned legal issues, especially those related to credibility (Jansen 2013, 1). Although the recognition of sexual orientation and gender identity persecution on the ground of the membership of a particular social group is established, it does not mean that other grounds should not be considered (Cragnolini 2013, 100). In fact, this legal expedient is the result of jurisprudential application, while UNHCR has addressed

[7] UNHCR, 2012: para 45: "*The two approaches – 'protected characteristics' and 'social perception' - to identifying "particular social groups" reflected in this definition are alternative, not cumulative tests*".

[8] Article 10(1)(d) of the Qualification Directive: "*[...] a group shall be considered to form a particular social group where in particular: - members of that group share an innate characteristic, or a common background that cannot be changed, or share a characteristic or belief that is so fundamental to identity or conscience that a person should not be forced to renounce it, and - that group has a distinct identity in the relevant country, because it is perceived as being different by the surrounding society [...]*".

[9] Article 21(1) EU Charter: "*Any discrimination based on any ground such as [...] sexual orientation shall be prohibited*".

this area only at a later stage.[10] Consequently, the fact that a case cannot fall within the scope of "particular social group" does not automatically mean that the person is not entitled to protection. International refugee law in this field is still evolving (UNHCR 2008, para 2); hence, LGBTI asylum cases should be researched systematically, so to identify new avenues and compare legal solutions. Particularly, dialogue and exchange should be fostered both in a vertical sense (international - regional level and regional – national level) and in a horizontal one (among different national systems). Both dimensions are important for the EU, since asylum law should be applied in a manner that is consistent with international refugee law and homogeneous within EU countries.

Tackling procedural gaps through the adoption of a LGBTI-sensitive approach

Proposals to close procedural gaps regarding credibility and evidentiary matters should take into consideration both the short and the long terms, as they should try to foresee problematic issues and be sensible to future developments.
To this extent, three points are crucial. First, asylum interviewers need to be specifically trained to deal with LGBTI applicants, taking into consideration the importance of '*cross-cultural competence*' (LaViolette 2013, 197). The ability to understand different cultural backgrounds without adopting judgemental attitudes avoids recurring to stereotypes, since it empowers the examiner's knowledge and expands the range of available tools. It also favours a positive attitude towards diversity, thus creating a safe environment for LGBTI people (UNHCR 2012, para 60).
Second, since facts on the situation of LGBTI people are often lacking or unreliable (UNHCR 2012, para 66), robust country of origin information should be collected and exchanged, particularly at the EU level. In this sense, cooperation among institutions, academics and non-governmental organisations must be encouraged, as different expertises can analyse different aspects, such as the legal situation, the perception of diversity and the cultural mindset.
Finally, the assessment of LGBTI cases should not focus on the demonstration of the applicants' sexual orientation, but rather on the proof of the fact that persecution is put in place because of their sexual orientation and/or gender identity. (UNHCR 2012, para 62). This would avoid intrusive questions regarding sexual practices, which are against the right to private life as enshrined in Article 7 EU Charter.[11] Furthermore, attention should be paid to the coherency of the applicant's narrative, at the same time keeping in mind the difficulties and the fear in disclosing one's intimate life.

The UNHCR Heightened Risk Identification Tool (HRIT)

The HRIT[12] is the UNHCR's instrument aimed at better identifying people who are at greatest risk in the context of resettlement. In a nutshell, it is composed of a list of questions and statements that guide the interviewer towards those elements worth of immediate and specific attention when dealing with vulnerable people.[13]
The HRIT latest edition (2010) includes LGBTI people as a target group (UNHCR 2010, 4). They fall under the '*legal and physical protection*' risk category: belonging to a sexual minority is explicitly considered among the risk indicators (UNHCR 2010, 10). Other indicators can be useful, such as the sexual and gender-based violence risk or the rejection by the community due to the '*transgression of social mores*' (UNHCR 2010, 10). Even though the HRIT cannot be seen as the panacea, it can indeed represent an important step towards the prioritisation of LGBTI people's claims, because it acknowledges their high vulnerability and reduce risks of overlooking important elements related to the legal situation and the personal safety.
It should be worth considering adopting a similar tool within the EU context; not only would it enhance LGBTI people's visibility, but it would also constitute a uniform role model to guide asylum adjudicators.

Conclusion

Many problems are still to be addressed in the context of LGBTI asylum claims and both qualitative and quantitative research need to be undertaken especially regarding the EU. As for credibility and burden of proof, future research should adopt an analytical approach to asylum decisions, linking domestic, regional and international case law. Through the application of an inductive methodology, studies should aim to identify best practices and draft guidelines to be adopted homogeneously by EU countries. This would be in line with the creation of a common asylum system and would create the bases for a mutual recognition of decisions.
Eventually, a proper approach to LGBTI asylum claims can also boost the awareness and the protection of LGBTI rights, both in countries of origin and destination. Emphasising the human rights dimensions of these asylum applications has the merit to link the respect for one's sexual orientation and gender identity to the core concept of human dignity, thus putting aside culturally-rooted justifications for abuses.
In this sense, future research should analyse the implementation of the '*Yogyakarta Principles on the Application of International Human Rights Law in relation to Sexual Orientation and Gender Identity*' within the context of refugee law. As for now, it seems that these principles have a great potential to advance LGBTI people's human rights, providing a sensitive interpretation of international human rights law.[14]

[10] In 2001 and expressly in 2008.

[11] See ICJ, 2014: 7.

[12] See UNHCR information: http://www.unhcr.org/4cd417919.html [Accessed 30 May 2015].

[13] Such as elderly people or women and girls.

[14] "*The Yogyakarta Principles reflect binding international legal standards*", UNHCR, 2008: para 9.

References

Carrol, A. and Paoli Itaborahy L. (2015) State-sposored homophobia. A world survey of laws: criminalisation, protection and recognition of same-sex love, ILGA, Available from http://old.ilga.org/Statehomophobia/ILGA_State_Sponsored_Homophobia_2015.pdf [Accessed 29 Mary 2015].

Charter of Fundamental Rights of the European Union, 30 March 2010, 2010/C 83/02, Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF [Accessed 29 May 2015].

Cragnolini, G. (2013) Lesbian, gay, bisexual and transgender refugees. Challenges in refugee status determination and living conditions in Turkey. In Thomas Spijkerboer (ed.) *Fleeing Homophobia. Sexual Orientation, gender identity and asylum*, London and New York: Routledge, 98-120.

Edwards, A. (2014) *X, Y and Z: The "A, B, C" of Claims based on Sexual Orientation and/or Gender Identity?*, Available from http://www.refworld.org/docid/53bb99984.html [Accessed 29 May 2015].

International Commission of Jurists (2014) *X, Y and Z: a glass half full for "rainbow refugees?*, Available from http://www.refworld.org/docid/538dca6f0.html [Accessed 29 May 2015].

International Lesbian, Gay, Bisexual, Trans and Intersex Association (2015) *76 countries still place criminal sanctions on homosexuality*, Available from http://dayagainsthomophobia.org/44-of-world-population-still-lives-under-criminal-sanctions-for-homosexuality-report-reveals/ [Accessed 29 May 2015].

Jensen, S. and Spijkerboer, T. (2011) *Fleeing Homophobia. Asylum claims related to sexual orientation and gender identity in Europe*, Amsterdam: COC Nederland – Vreje Universiteit Amsterdam, Available from http://www.refworld.org/docid/4ebba7852.html [Accessed 29 May 2015].

Jansen, S. (2013) Introduction. Fleeing homophobia, asylum claims related to sexual orientation and gender identity in Europe. In Thomas Spijkerboer (ed.) *Fleeing Homophobia. Sexual Orientation, gender identity and asylum*, London and New York: Routledge, 1-31.

LaViolette, N. (2013) Overcoming problems with sexual minority refugee claims. Is LGBT cultural competency training the solution?. In Thomas Spijkerboer (ed.) *Fleeing Homophobia. Sexual Orientation, gender identity and asylum*, London and New York: Routledge, 1-31.

Middelkoop, L. (2013) Normativity and credibility of sexual orientation in asyum decision making. In Thomas Spijkerboer (ed.) *Fleeing Homophobia. Sexual Orientation, gender identity and asylum*, London and New York: Routledge, 155-75.

O'Flaherty, M., and Fisher, J. (2008) Sexual Orientation, Gender Identity and International Human Rights Law: Contextualising the Yogyakarta Principles, *Human Rights Law Review*, 8 207-48.

The Yogyakarta Principles on the Application of International Human Rights Law in relation to Sexual Orientation and Gender Identity, March 2007, Available from http://www.yogyakartaprinciples.org/principles_en.htm [Accessed 29 May 2015].

United Nations Convention Relating to the Status of Refugees, 1951, Resolution 2198 (XXI), Available from http://www.unhcr.org/3b66c2aa10.html [accessed 29 May 2015].

United Nations High Commissioner for Refugee (UNHCR) (2008) *Guidance note on refugee claims relating to sexual orientation and gender identity*, 21 November 2008, Available from http://www.refworld.org/docid/48abd5660.html [Accessed 29 May 2015].

UNHCR (2010) *Heightened Risk Identification Tool*, Available from http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=4c46c6860 [Accessed 30 May 2015].

UNHCR (2010) *Heightened Risk Identification Tool – User Guide*, Available from http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=46f7c0cd2 [Accessed 30 May 2015].

UNHCR (2012) *Guidelines on International Protection n. 9. Claims to Refugee Status based on Sexual Orientation and/or Gender Identity within the context of Article 1A(2) of the 1951 Convention and/or its 1967 Protocol relating to the Status of Refugees*, 23 October 2012, HRC/GIP/12/09, Available from http://www.unhcr.org/509136ca9.pdf [Accessed 29 May 2015].

UNHCR (2013) Beyond Proof. Credibility assessment in EU Asylum Systems, Available from http://www.unhcr.org/51a8a08a9.pdf [Accessed 30 June 2015].

UNHCR (2015) *2015 UNHCR regional operations profile – Europe*, Available from http://www.unhcr.org/pages/4a02d9346.html [Accessed 29 May 2015].

RISING INSECURITY IN WEST AFRICA: BOKO HARAM IN FOCUS

Afua Boatemaa Yakohene
Research Fellow at the Legon Centre for International Affairs (LECIAD), University of Ghana, Legon and PhD Candidate in Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa, Italy
a.yakohene@sssup.it

Abstract

The West Africa region is currently grappling with insecurity due to terrorist acts, threats and tensions that the attacks of Boko Haram (BH), an extremist Islamist group, is unleashing primarily in Nigeria, with ripple effect in Niger, Cameroon and Chad. With the objective of creating an Islamic State first in Nigeria, BH is engaged in bombings, killings, and abductions. An integrated military approach comprising of Nigeria, Cameroon, Niger, Chad and recently Benin, are mounting counter attacks to quell the insurrection of BH. This paper argues that the adopted military approach particularly under ex-President Goodluck Jonathan was inadequate to addressing the long-term impact of the security of West Africa.

Keywords

Boko Haram, insecurity, Nigeria, development.

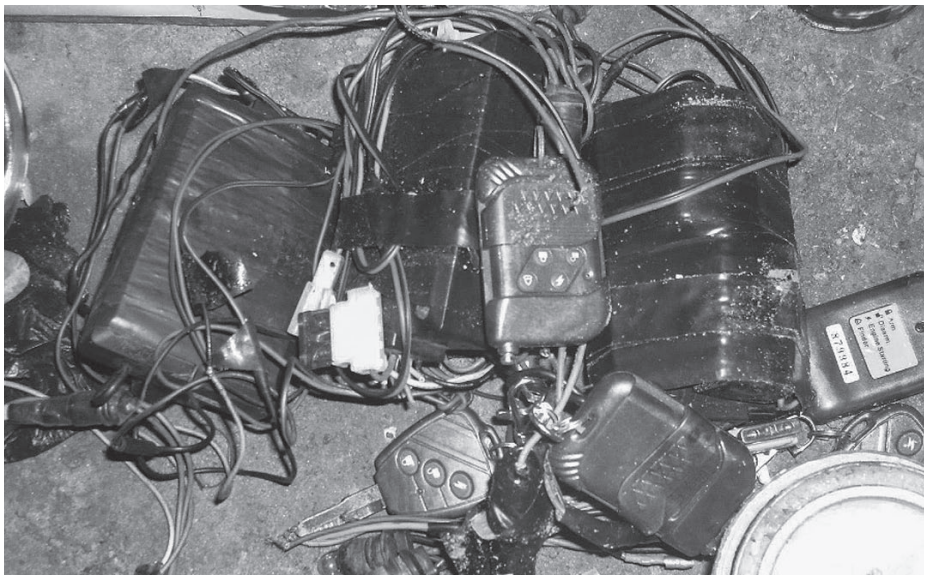
Introduction

Insecurity as intimated by Béland (2007) is "the state of fear or anxiety stemming from a concrete or alleged lack of protection." The degree of insecurity is affected by the changes in life situations. Security is therefore a core value of human life that cause an individual or a community to be untroubled by danger or fear.

Africa has been saddled with elements that have ushered in insecurity and posed threats to their human security and West Africa has not been left out of this equation. Intra-state violent conflicts, political instability, underdevelopment, corruption, poverty, starvation, epidemics and diseases among others have characterised the sub-region. Due to the happening and presence of these unfavourable elements, the sub-region has a tag of fragility to an extent. Some of these elements took the efforts and commitment of other States and international organisation for their effective management and resolution.

In West Africa, the Federal Republic of Nigeria is a dominant power. Nigeria's population is estimated to be about 178.5 million people making her the most populated country in Africa. It has an evenly split population of Christians and Muslims, with Christians largely in the Southern and Central parts of the country, and Muslims mostly in the Northern and South-Western regions. Nigeria is a force to reckon with in the region due to the economic and political clout it welds.

Adesoji (2010) expounds that Nigeria has had it bout with communal conflicts and ethno-religious violence. This extends from the Maitatsine religious disturbances in parts of Kano and Maiduguri in the early 1980s; to the JimetaYola religious disturbance (1984), 2 Ango Katof crisis in Kaduna State (1992); Bulumkutu Christian-Muslim riots (1982), Kaduna polytechnic Muslim-Christian skirmishes (1981-1982), and lastly to the 2009 BH uprising which is the subject of this paper. Nigeria has also had periods of political instability and is currently battling political and socio-economic issues such as unemployment, corruption, weak governance and perceived indifference on the part of politicians to the needs of Nigerians. Nonetheless, the current



insecurity Nigeria faces as a result of the activities of BH threatens the security, stability and development of the State, its citizens and that of its neighbouring countries namely Cameroon, Niger, and Chad.

The paper looks at who BH is and the genesis of its activities and the drivers and effects of BH's attacks on Nigeria and her neighbours, and criticises the effectiveness of national, regional and international efforts geared towards quelling the attacks and might of BH's.

Who Boko Haram is

Founded in 2002, the group's official name is Jama'atu Ahlis Sunna Lidda'awati wal-Jihad, meaning "People Committed to the Propagation of the Prophet's Teachings and Jihad" in Arabic. However, it is alleged that residents in the North-Eastern city of Maiduguri, where it had its headquarters, dubbed it BH which is loosely translated from Hausa language to mean "Western education is forbidden". Initially focused on opposing Western education, BH launched military operations in 2009 with the intention of creating an Islamic state. It declared areas it controlled such as Yobe, Borno, Kaduna, Gombe, Bauchi and Kano as a caliphate in 2014. Although most of BH's territory has been recaptured through successful counter attacks by the Nigerian Army and troops from Cameroon, Niger and Chad, sparse attacks on communities and the Nigerian Army by BH has been continuing. BH has become a thorn in the flesh of Nigeria, its neighbours and a cause of worry to the international community due to its confirmed relationship with international terrorist groups such as the extremist Islamic State (ISIS) currently fighting for the control of Iraq and Syria, Al Qaeda in the Islamic Maghreb and Al-Shabaab in the Horn of Africa.[1]

The Drivers and Effects of the Conflict

Crowley et al (2013) assert that BH was able to win the hearts of some Muslims because of social, economic and historical factors. For instance, political marginalisation, income inequality, inadequate public services, corruption, weak state control, mistrust of the security forces and heavy-handed security measures alienated the Central Government from the people and contributed towards BH's ability to recruit in Nigeria and from its neighbours and the establishment of its support base. Since 2009, BH carried out a spate of growing and indiscriminate terror attacks killing and injuring thousands of innocent civilians, police and military officers, public officials, opposing Muslim clerics and even their own group members. Thousand of residents have been internally displaced and others are refugees in neighbouring countries. Many freed girls and women recount numerous stories of how they were beaten, mutilated, used

[1] Smith-Spark, Laura, 'Islamist extremism rears its head across swath of Africa', CNN, viewed 20 March 2015, <http://edition.cnn.com/2015/03/19/africa/africa-islamist-extremism/index.html>.

as human shields, forcefully married and impregnated by BH forces among others.[2] Karmon[3] posits that BH targets include government buildings, churches, schools, politicians, police stations, newspapers, markets and banks through tactics such as antics drive-by shootings on motorcycles, suicide bombings, kidnapping and training of child soldiers starting in 2010.

The terror attacks are promoting different forms of insecurity, for example sectarianism between people of Islamic and Christian faith, increasing the economic inequality that exist between the Northerners and the Southerners, poverty, disease, orphans, lack of access to basic needs and employment and curtailed education.

National, Regional and International Efforts

Inasmuch as the erstwhile Nigerian President Goodluck Jonathan recognised that the militancy and criminality of BH posed as a threat to its national unity and territorial integrity, the disposition of his administration to quell and repress the insecurity that the atrocious activities of BH brought in were quite ineffective and unsustainable and portrayed an image of indifference on some occasions. According to Agbiboa, this involved political dialogue with all stakeholders and established a committee of inquiry to identify the grievances of the sect and make possible recommendations on how to improve security in the northeast region. Curfews, roadblocks, and state of emergency were declared on towns such as Borno, Adamawa, and Yobe. Programmes that addressed poverty, unemployment, social injustice and public corruption were embarked upon as these social evils were conditions that incited extremist tendencies among Northerners. The Government's attempt to grant amnesty to BH members was rejected by its current leader Abubakar Shekau and attempts to negotiate in a non-violent manner also backfired. The establishment of a special Joint Task Force (JTF), known as "Operation Restore Order (JTORO)" to eliminate the threat posed by BH recorded somewhat modest successes. Largely, the JTF has been accused of killing innocent people in the name of counter-terrorism, resorted to extralegal killings, dragnet arrests and use of intimidation techniques on unfortunate residents. These has further alienated the citizens from the State and its security forces.

Sub-regionally, Karmo intimates that, the other countries, Cameroon, Niger and Chad were compelled to involve their troops, logistics and financial resources in the combat against BH forces because its terrorist activities extended into the Northern tip of Cameroon, South-Western Chad and North-Eastern Niger. Also, documents found on some bodies of dead militants in Maidiguri indicated that many of them had come from Niger and Chad and fleeing BH fighters escape into the three countries.

The efforts and support of the Economic Community of West African States (ECOWAS) and African Union (AU) is alleged to be in the form of meetings only that seek to implement appropriate steps to counter BH and ensure civilian security. These efforts have been seen as a failure because ECOWAS is yet to come up with a prudent military strategy and financial assistance, which are needed to address the conflict. However, the ECOWAS Commission has dismissed accusations that it has failed to maintain regional stability in the face of BH's escalating attacks.[4] Also, an African Union plan to set up an 8000-strong multi-national regional force to fight the insurgents has not yet been implemented.[5]

Seeing the impact of terrorist activities on the international plane post 9/11, other actors outside the African continent are playing diverse crucial roles to address the rising insecurity in West Africa. The United States of America (USA) foreign policy on BH is clear, designating BH as a foreign terrorist organisation on 14th November, 2013, under Executive Order 13224. Since June 2013, the U.S. government has offered US$23 million worth of rewards for information on key leaders of terrorist organisations in West Africa and Abubakar Shekau heads the list with a reward of $7 million for information leading to his location. The USA Justice and Treasury Departments are also collaborating with counter-terrorism partners to investigate and prosecute terrorist suspects or supporters in the USA. USA's counterterrorism support to Nigeria includes building critical counterterrorism capabilities among Nigeria's civilian and law enforcement agencies to investigate terrorism cases, effectively dealing with explosive devices, and securing Nigeria's borders premised on respect for human rights and the rule of law; holding Regional Security working group meetings; the US State Department's Counterterrorism Finance (CTF) programme provides training that aims to restrict BH's ability to raise, move, and store money. Along with its neighbouring countries, Nigeria also participates in larger regional training opportunities such as combat medical, military intelligence, communications and logistics training with other Trans-Sahara Counterterrorism Partnership nations such as Algeria, Burkina Faso, Cameroon, Chad, Mali, Mauritania, Morocco, Niger, Senegal, and Tunisia.[6]

The European Union (EU) has expressed readiness and support to partner with the UN, AU, regional organisations, the individual states concerned and the

[2] Ndhlovu, R, 'I was flogged daily:' Rescued Boko Haram survivors share tales of horror', CNN, viewed 14 May 2015, < http://edition.cnn.com/2015/05/14/opinions/boko-haram-survivors-share-tales-of-horror/index.html>.

[3] Attacks between January 2012 – August 2013 included not only 50 churches and Nigerian Christians but also clerics or senior Islamic figures critical of Boko Haram and "un-Islamic" institutions or persons engaged in "un-Islamic" behaviour. According to a UN humanitarian agency, attacks between May and mid-December 2013 killed more than 1,200 people exclusive of killed insurgents. See Karmon, E. 'Boko Haram's International Reach', *Terrorism Research Initiative*, Vol 8, No. 1 (2014), viewed [2] June 2015, <http://www.terrorismanalysts.com/pt/index.php/pot/issue/view/ISSN%202334-3745>.

[4] Quartey, Lawrence 2012, 'ECOWAS brushes aside Boko Haram criticism', The Africa Report, 10 February 2012, viewed 1 June, 2015, <http://www.theafricareport.com/West-Africa/ecowas-brushes-aside-boko-haram-criticism.html>
US Department of State, 'Boko Haram and U.S. Counterterrorism Assistance to Nigeria', Fact Sheet, Office of the Spokesperson, Washington, DC, May 14, 2014, viewed June 2 2015, < http://www.state.gov/r/pa/prs/ps/2014/05/226072.htm>.

[5] Boko Haram fight 'hampered by poor Chad-Nigeria co-ordination', 12 May 2015, viewed 30 June 2015, < http://www.bbc.com/news/world-africa-32703833>.

[6] US Department of State, 'Boko Haram and U.S. Counterterrorism Assistance to Nigeria', Fact Sheet, Office of the Spokesperson, Washington, DC, May 14, 2014, retrieved June 2, 2015, < http://www.state.gov/r/pa/prs/ps/2014/05/226072.htm>.

Global Counter-Terrorism Forum (GCTF) to provide support with its full range of instruments, including the possibility of recourse to the African Peace Facility and EU crisis management tools. The French military and African Union States' forces intervention in Mali since January 2013 has provided new opportunities for the internationalisation of BH's activity and has brought it closer to other jihadist groups and presented it with possibilities for training, combat experience and operational cooperation with these organisations.[7]

This paper argues that although the strength of BH appear to have been reduced as a result of sustained strong coalition counter attacks, a high sense of insecurity is present in West Africa due to the sporadic attacks on North-Eastern communities and neighbouring countries which must be finally quelled. The ability of the coalition forces to reduce the strength of BH in a considerably short time, raises the question as to why BH was allowed to create insecurity for so long? Earlier attempts to resolve the conflict were unproductive because Nigeria had poorly trained and uncommitted troops who lacked financial, logistics and weaponry resources. It is believed that one of the main difficulties for the Nigerian security forces in patrolling its border with Cameroon is a lack of infrastructure. This enables BH to set up bases and training camps in the desert or forested areas of the Northern Nigerian-Cameroon border region.

Contrastingly, although her supporting neighbours seemed to be better resourced, equipped and trained there was an obvious lack of communication, coordination and command structures. Initially, the Nigerian Government appeared to be refusing offers of military assistance from other States. On many occasions, some political leaders and commanding officers of the neighbouring states complained of being alienated from the Nigerian Government and Army; and they were also inhibited from attacking a city or fully capturing it and maintaining a presence there.[8] This resulted in distrust and misunderstandings, which stymied preparations for the establishment of a regional force and led to a delay in pushing out BH's forces into the Sambisa forest and other parts of Nigeria and Cameroon. For example, Chad was compelled to take unilateral action in January 2015, which allowed it to pursue terrorists into Nigeria, after BH's violence started to choke off imports to its economy.

A question that begs to be asked is, was the initial lack of cooperation from Nigeria due to the fear of appearing disarmed, incompetent and unable to protect its citizenry and territorial integrity? Or rather, was the desire to re-gain power in the erstwhile 28th March, 2015, general elections a motivating factor in its latter proactive disposition? The study is more inclined towards the latter question as the intensity of the coalition attacks and Nigerian army resilience seem to have reduced after President Jonathan was defeated in the Presidential election by the newly sworn-in President Muhammadu Buhari. President Buhari has embarked on a closer and more defined relationship with its neighbours and brought Benin into the fold by meeting its leaders, released money to the Nigeria Army to be better prepared and also directed the relocation of the military command and control centre from the capital Abuja to Maiduguri, the main city at the heart of the insurgency, until the conflict is resolved.

ECOWAS' non-commitment to the crisis could be a portrayal of the fragility of the sub-region as a result of on-going internal economic, social, political difficulties in member states, thus the hesitation to be fully involved. It could also stem from fear of reprisals from BH supporters and sympathisers in their individual states especially seeing that the reasons that gave room for BH's radicalisation and growth still exist in Nigeria and in the neighbouring states.

Conclusion and Recommendations

The sporadic attacks of BH on the Nigerian army, some towns and neighbouring countries is a clear indication that it posses the ability to kill, cause mayhem and make individuals and countries insecure. It is disappointing that the atrocious effects of BH's power and activities were not effectively addressed earlier. Lack of resources, untrained and uncommitted Nigerian troops, the absence of a ready regional force and speculated political reasons have been cited as reasons that inhibited this possibility and allowed issues to spiral out of control thereby creating the current insecure environment Nigeria and West Africa as a whole is situated in. The lack of concrete decisions and actions of ECOWAS and the AU to address the rising insecurity posed by BH could be a reflection of either their decreasing ability and commitment as a group due to structural and financial challenges or individual member states' internal challenges that are negatively influencing that of the two regional groups. For a sub-region such as West Africa that is beset with many challenges, this is an unwelcome blow with dire consequences on its current and long-term security, stability and development.

The future security of Nigeria and the sub-region lies in consensual, well-coordinated, well-structured and well-resourced interventions by national and regional forces. The overall success in resolving the BH threat calls for sustained measures aimed at intricately addressing the social, economic and political issues that galvanised terrorist radicalisation and gave BH a foothold in Nigeria. This would help reduce the level of poverty, income inequality, mistrust of the Government, bring in more and better public services and ultimately break the hold of BH over Northern Nigeria. These must be equally carried out in Cameroon, Niger, Chad and Benin as they have almost the same prevailing issues and efforts to address them now would have long-term security, stability and development benefits.

[7] Council of the European Union, 'Council conclusions on the Boko Haram threat', Foreign Affairs Council Brussels, 9 February 2015, retrieved June 2, 2015, <http://www.consilium.europa.eu/en/press/press-releases/2015/02/150209-council-conclusions-boko-haram-threat/>.

[8] Harding, Luke, 'Nigeria's prospects for defeating Boko Haram look bleak', The Guardian, 22 January 2015, viewed 15 April 2015, < http://www.theguardian.com/world/2015/jan/22/nigeria-prospects-defeating-boko-haram-look-bleak>.

References

Adesoji, A. (2010) The Boko Haram Uprising and Islamic Revivalism in Nigeria, *Africa Spectrum*, 45, (2), 95-108.

Agbiboa, Daniel E. (2013) No Retreat, No Surrender: Understanding the Religious Terrorism of Boko Haram in Nigeria', *African Study Monographs*, 34 (2): 65–84, August 2013, pp. 65-66.

Béland, D. (2007) Insecurity and Politics: A Framework, *Canadian Journal of Sociology/Cahiers canadiens de sociologie*, 32(3), p. 320.

Crowley, R. and Wilkinson, H. (2013) Boko Haram: A New Threat in West Africa', in OECD, *Conflict over Resources and Terrorism: Two Facets of Insecurity*, OECD Publication, pp. 99-112.

Karmon, E. (2014) Boko Haram's International Reach', *Terrorism Research Initiative*, Vol. 8, No. 1, pp. 74-83.

PREVENTING AND COMPETING ELECTORAL FRAUD MEASURES EMPLOYED BY THE IRAQI INDEPENDENT HIGH ELECTORAL COMMISSION (IHEC)

Ali Al-Bayati
PhD Candidate
Politics, Human Rights and Sustainability Programme,
Sant'Anna School of Advanced Studies, Pisa (Italy)
a.albayati@sssup.it

Abstract

This paper sheds light on some of the adopted measures by the Iraqi Electoral Management Body (EMB) to prevent electoral fraud during 2013 Governorate council elections. It also suggests a set of recommendations to improve that process during the future electoral event.

Introduction

Even long-established democracies around the world are not exempt from the occurrence of fraud, which will undermine the public trust in elections whenever it occurs. Significant allegations of fraud tainted the 2009 and even the 2014 presidential elections in Afghanistan (Al-SharqAl-Awast, 2014) and several other countries around the world. This raises many concerns for the International Community that, in response, deployed many observation teams, in an attempt to prevent fraud and ensure the legitimacy of elections, in countries that newly adopted democratic means of peaceful transition of power.

Thishighlightedapotentialvulnerability to fraudulent activities with respect to all aspects of the election process, including the processes of voter registration, electoral campaigning, polling, counting and, finally, the announcement of results.

Free, fair and competitive elections are essential for any 'new' or old democracy in terms of providing public accountability, transparency,

and representation in general (Alvarez, 2008). This is particularly important in a diverse and highly charged political environment such as that in Iraq.

The main purpose of this paper is to identify some of the anti-fraud measures adopted by the Independent High Electoral Commission (IHEC) for the Governorates Council Elections (GCE) in 2013 in particular, as well as its general anti-fraud measure in place for electoral events. In addition, the purpose of the analysis is to identify additional measures the IHEC could use to counter fraud in future electoral events.

This paper is based on number of meetings with IHEC officials as well as review of electoral law and regulations issued by the IHEC for the April 20, 2013 Governorate Council Elections (GCE).

Photo: IHEC staff auditing some ballot boxes looking for potential electoral fraud during 2013 Governorates council elections in Iraq.

The paper analyses the procedures in place at the time of writing (June 2013). These procedures, such as the polling and counting procedures and the electoral complaints procedures, were amended several times during the preparation for the elections prior to the GCE. This paper takes into account the most updated procedures.

1. What is Electoral Fraud?

A variety of definitions of 'electoral fraud' are available. The broader approach defines Electoral Fraud as a violation of the 'principles of free and fair elections and the right of the citizens to choose their representatives'. A narrower approach defines it as a violation of 'the domestic laws governing elections in a country article " (Vickery, 2012)
The International Association of Electoral System (IFES) published a series of white papers concerning Electoral Fraud which

suggest that fraud is a 'deliberate wrong-doing by elections officials or other electoral stakeholders, which distorts the individual or collective will of the voters'

(Vickery,2012). IHEC's definition of election fraud is provided by IHEC regulation No. 14 /2008, which defines fraud as "*Do or refrain from doing all what can be considered a confront to the provisions of the GCE electoral law number 36/2008*".
In addition to the aforementioned regulation, the anti-fraud measures specific to each activity, i.e. each step in the electoral process, are codified in the respective procedures for that process. Thus, for example, the anti-fraud measures for the polling and counting process are outlined in the polling and counting procedures (IHEC, 2013).

The methods to detect electoral fraud span the entire spectrum of the electoral process. Below is an overview of the approaches for electoral fraud detection as outlined in the IHEC procedures.

2. Anti-fraud measures during polling and counting Polling ballots, boxes, and stamps

Highly-qualified printing companies printed the ballot papers and security features were incorporated into the design of the ballots to prevent reproduction (Al-Hiti, 2013).
The number of ballots issued to individual polling stations was closely monitored to ensure that any discrepancies could be easily detected. The ballots were produced in 50-ballot pads and had sequential serial numbers to enable close tracking should a pad go missing or be fraudulently used. However, individual ballots issued to voters were not able to be tracked to ensure the secrecy of the vote (Abdulilah, 2012).
Special numbered seals were used on the ballot boxes with the numbers recorded on special forms during the opening and closure of polling and were checked before counting began. Any discrepancy was recorded and an investigation would be initiated, which might result in the ballot box and its contents being excluded from the results. Observers and entity agents could also record these numbers and report any discrepancy. Tamper-Evident Bags (TEBs) were used to store sensitive information regarding the election and tally sheets to ensure that misuse could be detected.
All ballots were counted and displayed in front of accredited observers and entity agents and were 'double counted' (Abduilah, 2012) to ensure accuracy. This double count also applied to the number of voters that signed the voters' list.

Indelible Ink.

Voters were 'marked' with indelible ink to show that they had voted and to prevent multiple voting.
Apart from voters who had lost both hands, all voters had to have their right index finger marked before voting and the ballot box monitor would ensure that the nail was covered and the voter did not wipe his finger before the ink dried. The polling staff made sure the ink bottle was shaken to make the indelible ink more effective (Abdulilah, 2012)
After closing polling activities at the end of the day, the polling station manager would collect all blue pens, the seal and the indelible ink inside a TEB to prevent any illegal voting and 'deliberate ballot spoiling' by the polling staff after closure of the polls.

Votes made by polling staff, observers and political parties agents

Polling staff were allowed to vote in the same polling station if their names were not registered at other stations in the same centre. The observers and political party agents were not allowed to vote at the polling station where they acted as observers unless they were registered at that station (IHEC, 2013).

Staffing

Only IHEC staff was allowed access to sensitive election materials. Voters were informed exactly what to expect and what they should on entering a polling station by the IHEC polling staff recruited by the Ministry of Education (MoE). The personnel, who included professional teachers, had extensive training with respect to polling procedures. All IHEC staff signed a Code of Conduct, which, if breached, might result in significant professional consequences[1].
In addition to all polling staff, IHEC hired around 700 'monitors' from the MoE and lawyers to monitor the polling process and report directly to the IHEC in the event any violations occurred in their areas of competence.

[1] Al-Hiti, 2013.

Special Voting procedures - Military, Police, Detainee and Hospital Voting

Procedures have been developed to allow certain categories of voters who were working on the Election Day or unable to attend a polling station to be given the opportunity to vote. This includes members of the security forces.
For the military and the police forces, the IHEC conducted special voting sessions seven days before the Election Day. The IHEC created a special voting list based on information obtained from the Ministry of Interior (MoI) and Ministry of Defence (MoD). The names of the Iraqi Security Forces (ISF) voters were removed from the regular voter register to prevent any opportunity for multiple voting. For this purpose the IHEC had to cross-check its data with lists provided by the MoD and the MoI. In that process the IHEC could not locate 46,000 names due to insufficient information provided by the relevant ministries (Al-Waely, 2013). This led to exclusion from special voting and the individuals in question were asked to participate in the regular voting process. Only members of the security forces working on election day were included in the special voting procedure.

Hospital patients and prisoners were given the opportunity to vote by conditional balloting. These voters were issued 'secrecy envelopes' in which they could place their ballot papers. The envelope was inserted into another envelope, with their name, number and governorate details recorded on the outside, and was placed into the ballot box.
The eligibility of this category of voter was confirmed during the counting process by checking the voter's data on the conditional ballot envelope against the voters' register. If a voter was not identified in the voter's register as eligible to vote in the governorate for which the voter had cast a ballot, then the vote would not be counted. Special Voters were also marked with indelible ink.

Counting

Counting took place at the polling stations after closure (except for special voting that occurred at the governorate count centres) in full view of observers and entity agents. Additionally, regular polling stations requiring an audit were checked at the governorate count centres and were counted if the problem was resolved.

Special procedures have been developed to count and compare all ballots cast with the number of voters per station and also to compare the total number of ballots accounted for with the number of ballots issued to a particular station. If a discrepancy exceeds 4%, an investigation was initiated and the ballot box could be excluded from further tallying of results.

Results from the polling-centre level were produced in order to accelerate the announcement of overall results. The political entities were provided with a copy of the results (Al-Waely, 2013). During the training of the polling-staff the IHEC explained the sanctions that were provided for by law with respect to any fraudulent activity committed by staff members. In addition, references to these sanctions were included in their contracts and the code of conduct.
The Board of Commissioners (BoC) authorized the (Chief Electoral Officer) CEO to install surveillance cameras to monitor the Governorates Electoral Offices (GEOs) Warehouses and Counting and Sorting Centres. However, there were no instructions regarding who would be responsible to check the recordings and whether the recordings would be used in an investigation if complaints were submitted.

The CEO is authorized by the BoC to relocate polling staff from one polling place to another to avoid using polling staff from the same neighbourhood. For this GCE, the BoC decided to relocate some GEO managers. The measure also involved the districts of Qadisia, Babil, Thi-qar, Muthana, Najaf and Baghdad-Rusafa.
All ballots were counted and displayed in front of accredited observers and entity agents. Observers and entity agents could record information from the count form and results sheet once the process was completed. Copies of the results form were displayed on the external wall of the polling station for one day.

All tally sheets were securely transferred to Baghdad for data-entry at the IHEC Data Entry Centre (DEC) under the full observation of political parties' agent-representatives-, national and international observers such as Arab league observer's, number of foreign embassies in Iraqi and other organizations . Data-entry during the tally process was carried out under full observation and a subsequent audit was used to investigate suspect results sheets. All of the original results forms were scanned and archived.

If the polling centre had a big hall, the counting for all the stations in that centre was conducted in that hall in the presence of all political party agents and observers. This measure addressed the possibility of a lack of political party agents and observers in some polling stations.

Recommendations

The polling procedures should regulate the use of mobile phones by voters, who should not be allowed to bring mobile phones to the polling station, as that may contribute to encouraging vote buying. The IHEC should approve the polling and counting procedures early enough to allow for fully-comprehensive
training of all polling staff and to make sure the procedures are clearly understood and applied.
Paper towels, sheets of paper and other cleaning materials should be either removed from the polling kits

or should be indicated to polling staff so that such items are not provided to voters, who may use them to wipe the indelible ink off their fingers before it dries.

3. Current anti-fraud measures at the Data Entry Centre (DEC)

The tabulation of results took place at the Data Entry Centre (DEC). The IHEC assigned around 1,100 staff members to work at the DEC (in two shifts from 8 am to 2 pm and from 2 pm to 8 pm) to execute all phases and processes concerning the definition of results and reconciliation forms –reconciling the number of the electoral materials been delivered to ee ach and every poling centre - at that centre level. In the staff-contracting process, the IHEC made efforts to ensure the representation of all-Iraqi - ethnic and religious components as an anti-fraud measure.

The DEC provided all necessary information to the IHEC Complaints Section concerning investigation and coordinated audit cases with all relevant count centres at the GEOs.

The data from each polling station was double entered simultaneously by two data-entry staff members in different sections of the DEC and to prevent any discrepancy between the two entries a visual check and audit followed.

The IHEC established that persons authorized inside the DEC would be the data-entry staff, a limited number of the IHEC staff, centre security personnel, accredited political parties agents, observers and the media.

Recommendations

The IHEC should introduce electronic triggers in the DEC software to highlight polling stations results that may be indicators of potential fraud.

The suggested cases to be highlighted are the following:

· Turnout of voters higher than 85% of registered voters at a given station and/or centre.

· Total number of votes for a single political entity and/or a candidate higher than 90% of the total votes cast in that station and/or centre.

· Total number of votes higher than 100%.

· Number of spoiled and/or invalid votes higher than an accepted percentage. The percentage can be determined based on statistics of disabled, illiterate, and assisted voters.

The above cases should be audited and investigated by the IHEC and results should not be included in the preliminary results. The data-entry process is a highly sensitive step in the electoral process and the IHEC should maintain a highly transparent procedure during all phases and make sure that the agents of political parties and observers can access all information in a way that does not interrupt the process.

4. Current anti-fraud measures in the processing of complaints and detecting fraud

In 2005, the IHEC adopted a so-called 'Categorization Process', according to which the complaints are categorized based on 'inspection outcome' (Lopez-Pintor, 2010). Important complaints receive 'red coding' and the IHEC cannot announce electoral results without deciding on these. Complaints with a 'green' coding require investigation but do not delay results. If the complaints are groundless, have no legal basis or are not relevant to the elections, they are categorized with a 'yellow' code and dismissed immediately.

As an anti-fraud measure for the GCE, the IHEC established three categorization committees chaired by the Commissioners. In addition to three members from the IHEC, each committee included one UN international assistance team member(Abed, 2013).

Only voters and agents – representatives - of political parties can submit complaints at all stages of the electoral process.

Complainants who have witnessed violations should submit complaints, using the forms available at all polling and counting centres as well as at the IHEC National Office and the GEOs (Abed, 2013). Each form has a serial number, allowing for proper follow-up on a given complaint, and contains three carbon copies. Carbon copies are given to the complainant and to the GEO complaints unit, while the original first page goes to the IHEC National Office, Complaints and Legal Section for assessment and a final decision.

The complaints should be submitted within 48 hours following the moment the polling activities are initiated. Unused complaint forms are to be retrieved from the National Office as one of the measures to avoid missing any complaints that have been submitted.

The complaints were registered in a manual and also an electronic register. A database was designed to keep track of all complaints for each GEO and was updated according to the investigation progress.

Recommendations

In order to ensure a more transparent complaints process, the IHEC should create a database of all complaints which is available to the public on the IHEC website. Permanent staff should be responsible for updating the database.

The categorization process should be centralized at the National Office level. Involvement of the Commissioners in this process is not necessary as the process requires technical skills and experience specifically related to complaints. Therefore, staff members with adequate experience should be involved and daily or weekly reports should be submitted to the BoC to keep them updated.

Training and internship opportunities at other Electoral Management Bodies (EMBs) should be provided to the legal staff in the national office and in the complaints units at the GEOs. Special fraud-detection and investigation training programs should be developed and provided to staff involved in the investigation process in order to ensure they acquire a full understanding of the complaints process from a broad prospective.

As the IHEC investigates and decides on complaints, greater autonomy should be afforded to the Complaints Section office and relevant units at the GEO level. All relevant departments of the IHEC should prioritize the complaints section's requests as this may contribute to the adjudication of complaints in a timely manner.

Previously, complaints were to be submitted within three days starting from the time the violation occurred (Al-Hiti, 2013), which was more reasonable than the current deadline.

The IHEC should not limit the period for individuals and organizations to file a complaint as this is a very important fraud-detecting measure.

Moreover, this will help to avoid giving the wrong perception to political entities and the public in general with regard to IHEC efforts in combating and detecting electoral fraud.

Conclusion

Electoral anti-fraud measures should be assessed, analyzed and reinforced before any elections. Establishing an ad hoc committee is not sufficient. As no archive for such measures is kept, the process will have to start always form scratch.

An anti-fraud unit should be established and attached to the BOC to keep all documentation and minutes from each committees and small permanent staff should be kept all the times. A special training program should be designed and regularly updated on how to detect fraud and investigate fraud cases.

Additionally, all relevant departments should participate in lessons learned activities after each election to assess the efficiency of the measures taken by IHEC to combat fraud.

References Papers

Al-Sharq Al-Awast. (2014) Afghan election results delayed amid fraud accusations. Available from www.aawsat.net [Accessed 30 July 2014]

Alvarez, Michael (2008) Election Fraud Detecting and Deterring Electoral Manipulation. Brookings Institution Press.

Darnolf, S. (2011) Assessing Electoral Fraud in New Democracies Available from www.ifes.org [Accessed 15 March 2013]

Lopez-Pintor, R. (2010) Assessing Electoral Fraud in New Democracies, Abasic Conceptual Framework. Available from www.ifes.org [Accessed 10 March 2013]

Vickery, C. &. (2012) Assessing Electoral Fraud in New Democracies: Refining the Vocabulary. Available from www.ifes.org [Accessed 30 March 2013]

IHEC Regulations and Procedures For Governorates Council Elections 2013

Independent High Electoral Commission (2012) Voting, Counting and Sorting Regulation, reg. 11.

Independent High Electoral Commission (2013) Polling and Counting Procedures.

Independent High Electoral Commission (2013) Counting and sorting centers procedures.

Independent High Electoral Commission (2013) Polling and counting Complaints.

Independent High Electoral Commission (2013) Special voting procedures.

Independent High Electoral Commission (2013) Special conditional voting procedures.

Independent High Electoral Commission (2013) Data entry center procedure.

Interviews:

1. Abed, A. H. Head of Legal Consultations and Complaints (2013). Intreviewed by Ali Al-Bayati on March, 10.
2. Al-Waely, W, Commissioner. (2013) Interveiwed by Ali Al-Bayati, on March, 20.
3. Al-Hiti, S. Comissioner (2013) Intervewed by Ali Al-Bayati on March, 20.
4. Shaghaet, K. A. The Deputy to the Chief Electoral Officer (2013). Interviewed by Ali Al-Bayati on March 13.
5. Abdullah, A, former Operations Department Manger (2013) interviewed by Ali Al-Bayati on April, 10.

Next Events & Trainings

For complete info about trainings, research & on going projects please refer to www.itpcm.dirpolis.sssup.it

Trainings/Education	When	Where	Application Deadline	Info & Contacts
The Master of Arts in Human Rights and Conflict Management	from January 2015	Pisa Italy		www.humanrights.sssup.it humanrights@sssup.it
Hostile Environment Awareness Training Course	HEAT Course III-2015: October 5-9, 2015 HEAT Course IV-2015: November 9-13, 2015	Leghorn Italy	(a) by September 14, 2015 for the Heat Course III-2015 at www.sssup.it/heat2015-III/application (b) by October 19, 2015 for the Heat Course IV-2015 at www.sssup.it/heat2015-IV/application	www.itpcm.sssup.it heat@sssup.it;
Civilian Peace Support Operations	31 August – 4 September 2015	Yaoundé, Cameroon	July, 15th 2015	Application available at: http://www.sssup.it/ist_context_elenco.jsp?ID_LINK=12902&id_context=53759&page=11&area=46 Applicants are required to complete an application form and email to fpeaces@gmail.com or pso_training@yahoo.com Dr. Melvis M. NDILOSEH (+237.77.63.63.23: Department of International Law, IRIC)
International Standards for the Protection of Individuals and Groups: A Training Course for Field Officers Working on Human Rights	12 - 20 November 2015	Addis Ababa, Ethiopia	September, 6th 2015	http://www.entriforccm.eu/training/specialisation-training-courses/human-rights-2.html itpcm@sssup.it

Scuola Superiore Sant'Anna
di Studi Universitari e di Perfezionamento

The ITPCM

Staff members & Contacts

Director

Prof. Andrea de Guttry
deguttry@sssup.it

Peace Keeping Branch

Rossella Altamura
Project Officer
ro.altamura@sssup.it

Matteo Bartolini
Project Officer
ma.bartolini@sssup.it

Annalisa Creta
Research Fellow
a.creta@sssup.it

Emanuele Sommario
Assistant Professor
esommar@sssup.it

International Disasters Response Branch

Matteo Bonfanti
Research Fellow
m.bonfanti@sssup.it

Francesca Capone
Research Fellow
f.capone@sssup.it

Enrica Pautasso
Project Manager
e.pautasso@sssup.it

Francesca Vietti
Research Fellow
f.vietti@sssup.it

Decentralised Cooperation Branch

Annarosa Mezzasalma
Project Officer
a.mezzasalma@sssup.it

Address

Via Cardinale Maffi, 27
56127 Pisa - ITALY
tel: +39 050 882685
fax: +39 050 882665

International Training Programme for Conflict Management 1995-2015, 20th Anniversary

itpcm@sssup.it - www.itpcm.sssup.it