

13th ICCRTS
“C2 for Complex Endeavours”
Terrorism online and the change of modus operandi
Topic 7: Network-Centric Experimentation and Analysis
Roland Heickerö, PhD
Adjunct Professor
Deputy Research Director
Swedish Defence Research Agency, FOI
Division of Defence Analysis
Gullfossgatan 6, Kista
SE-164 90 Stockholm
Sweden
Phone: +46 8 5550 38 25
E-mail: roland.heickero@foi.se

Abstract

One consequence of rapid technological change in an information society is that the socio-economical and technical systems become more vulnerable to information related threats. The cost of electronic and digital warfare is decreasing and at the same time knowledge about how to conduct information attacks is spreading to a large number of people due to the rapid growth of the Internet. Asymmetry is a characteristic, meaning that it is relatively cheap (generally speaking), to accomplish a cyber attack against a critical system such as SCADA (Supervisory Control And Data Acquisition). On the other hand, it is quite expensive to protect the same system from illegitimate influence.

The lower barriers mean that new types of actors, such as hackers, crackers, criminals and cyber terrorist will use information warfare tools to achieve certain goals. In order to reduce dangers and to act proactively it is important to gain knowledge and to develop strategies and tactics for counter action to handle new type of threats and risks in an open society. New methods are required for analysing the motives and driving forces of insurgents in an information arena.

The following paper initially discusses the term cyber terrorism and its logic in an asymmetric context. The insurgents' motives, driving forces, usage of information warfare means and weapons are shown. The methods a cyber aggressor could use to plan and conduct an operation and its effects and consequences are described in an *actor-target-effect chain*.

The transformations of modus operandi for cyber terrorism are discussed and exemplified by the case of al-Qaeda and by other terrorist organisations. The paper ends with a short conclusion.

1. Terrorism in cyberspace - general

Cyber terrorism is a part of information warfare and is a generic term that involves a number of hostile activities towards society with political, religious, ideological and/or ethnical aims. The purpose of an action is to disturb, distort, manipulate or destroy an opponent's critical information- and communication infrastructure, SCADA. Cyber terrorism is comprised of different types of means and methods such as computer network operations (CNO), electronic warfare (EW) and psychological operations (PsyOps).

More or less daily cyber attacks occur today: hacking, distribution of viruses, trojans and worms, password thefts et cetera. By using functionality providing denial-of-services (DOS) and spamming, it is possible to overload and saturate an opponent's servers in order to delay or interrupt communication. Qualified hackers outside an organisation or planted within it could perform industrial espionage.

Companies, authorities and individuals are exposed to exploitation and penetration campaigns. There are numerous examples of fraud attempts against important public systems such as bank accounts and information stored in databases. In some cases, the activities are quite harmless, in others considerably more serious and costly for the target. Incidents have been reported from Sweden and abroad where cyber terrorists may be the originators. For law enforcement authorities it is difficult to clarify the people and organisations behind an attack. Hence, it is not always possible to identify either the aggressor or the real purpose behind it.

The Internet makes it possible to act anonymously provided that the cyber antagonists have proper skills and knowledge of how to avoid digital tracing and computer forensics. The consequences so far, in terms of dead and wounded, have been very limited compared to the effect of traditional terrorism. However, a directed and qualified cyber attack against critical information systems could have great effects on society and could be lethal depending on what system is being attacked. To gain public trust it is essential for authorities to deal effectively with the situation in an upcoming cyber crisis.

Even if the cyber attack fails due to effective prevention techniques such as IDS¹ and others, it is important to realise that the aggressor may have collected valuable knowledge and information. Every attack, if it succeeds or not, exposes the target groups vulnerability, for instance what type of protection mechanisms and methods that are used by the defender. This is vital information in a any future operation. Hence, a cyber attack can be regarded as asymmetric in the sense that the target groups do not get any information about the aggressors own vulnerabilities or constraints.

¹ IDS – Intrusion Detecting System

Evidence shows that, over a period of time terrorists and other hostile actors develop methods and strategies for conducting electronic and digital attacks on a larger scale [1]. Especially dangerous and lethal will be the case when insurgents learn to use EW more frequently for instance against air traffic systems [2] and GPS. The costs for carrying out such operations are quite low but the effects would be massive. Collin [3] estimates that the number of cyber attacks will increase over a period of time. That implies that ordinary analysis models, used for monitoring traditional terrorist activities, have to be adjusted to the new information warfare threats, such as cyber terrorism. Therefore the methods have to be adapted to changes in insurgents' logic and modus operandi as well as attack patterns in the cyber arena, their usage of advanced IW-weapons², technological knowledge and organisational structures et cetera.

1.1 Actors and antagonist in cyber space

There is a discrepancy between actors and antagonists. Actors are individuals, groups and organisations that have the ability to conduct malicious activities but lack motives for doing so. Antagonists on the other hand, are groups that have the motives, resources and willingness to conduct operations of different kinds against specific targets. Over a period of time an actor could transform to an antagonist and vice versa.

The choice of organisational structure depends on objectives and goals, resources and the historical backgrounds of the insurgents. In order to fulfil a certain task the antagonist could be organised in a wide range of structures from hierarchical ones to adhoc-networks. The first could be an intelligence organisation, the latter a terrorist cell acting more or less autonomously depending on intention. Al-Qaeda, for instance, have a centralised command that decides overall goals but acts in a distributed and autonomous way at lower levels with a high degree of freedom of actions for the cell members. Some examples of different types of antagonists in the cyber arena are *script kiddies*, *crackers*, *hackers*, *hacktivists*, *cyber terrorists* and *insiders*.

Some decisive factors in determining whether an individual becomes a cyber terrorist in a specific situation are: personal motivation, risk acceptance, current personal circumstances, IT-skills, and ethical/moral limitations and restrictions. When planning an attack there is also some kind of economical and personal risk evaluation of whether the operation will succeed or not in relation to the potential cost of conducting the operation.

The term *cyber terrorist* can be divided into “pure” cyber terrorists and “traditional” terrorists using Internet for coordination of (physical) activities. The boundary between them is not sharp and tends to blur. Contrary to traditional terrorists the “pure” cyber terrorists wants to act anonymously on the

² IW – Information Warfare

Internet as well as to hide the real intention behind an info logical attack as long as possible. The Internet is both the tool and enabler of cyber attacks. For an insurgent, the nature of terrorism online is quite safe, beneficial and hard to detect compared to that of traditional terrorist action. The numbers of identified cyber attempts with a lethal outcome are low, so far. But cyber terrorists have tried to attack critical infrastructure with a varying degrees of success.

An *insider* could act as a cyber terrorist. This type of antagonist is by definition placed within an organisation. Such persons could act independently, without any support from outside. Driving forces for this category of individuals is discontent with the current situation and a feeling of unfair treatment from management and/or by co-workers. Redundancy processes and organisational cut backs could provoke the behaviour as well as economical benefits. Insiders, for instance individuals that hold terrorist sympathies in combination with good IT-skills, could also be planted in an organisation. The purpose and goal is to steal vital information, to put malware into control functions or to open up for future attacks. Such individuals apply for work in high tech companies, research agencies and public authorities etc. that are responsible for critical infrastructure. The consequences of insider activity can be serious.

1.2 Resources and means

The combination of resources together with motives, driving forces and current security situation, defines and steers possible antagonistic approaches. Compared to single individuals (stand alone) and smaller groups, Intelligence agencies for instance could supply and house large resources.

Resources may vary over time and comprise personal, economical and logistical resources as well as knowledge in and access to (IT and EW) weapons and networks. Some examples of cyber weapons are logical bombs, worms, viruses and trojans. Electronic warfare weapons could be used for monitoring and jamming mobile communication and navigation system GPS. By directed microwave pulses (EMP), electronic components could be destroyed.

As mentioned, there is a relation between cost and risk. The probability for an insurgent to conduct a qualified cyber attack depends on calculated costs and the risk of detection by digital tracking methods.

The Internet can in many cases provide manuals and instructions on how to either design IW tools or ways to purchase them. For instance it is possible to buy cheap EW-equipment for monitoring and jamming communication systems for a few hundred dollars. Sketches and blueprints are to some extent available on the Net. Compared to the Cold War era, sensitive information is no longer exclusively restricted to the intelligence and military sector but could be available to many people provided that they have the right knowledge and skills to find the information.

The barriers against antagonistic operations are likely to decrease over time due to continuing price-reductions in combination with easier access to information on techniques and procedures. It is possible, with small means, to affect critical infrastructure on a large scale, if the motives and willingness are right.

1.3 Targets, effects and consequences

In general, the cyber antagonist wants to act at a large distance from the target (if he or she is not an insider). The apparatus for doing so is quite simple and cheap. To carry out a malicious cyber operation it is enough to have an advanced computer and effective network connected to it. EW weapons may require more sophisticated equipment depending on purpose of the action.

In order to hide the intention of an operation and to avoid digital tracking, an antagonist could use closed peer-to-peer networks³ and bit-torrent-techniques⁴ for communication and information exchange. High level security could be achieved between members of a terrorist cell by using acceptance control and continuous approval. Ad-hoc networks are preferred in the sense that the network activates only when necessary and shuts down after the information exchange processes are finished.

By using modern network techniques it is also possible to gain information about objects to attack, to discuss suitable methods and to coordinate people and resources in time and space. The exchange process of sending and receiving important messages can be hidden in information files and on web sites e.g. steganography. Especially useful for this purpose, are sensitive web sites for instance those that contain pornographic material which can be used to hide information. It makes it hard for counter insurgents to find them.

Available target for attack depends on the purposes and resources of the insurgent. Information about interesting objects could be downloaded from the Internet describing placing of the target, what design and construction it has as well as methods to jam, intercept or to destroy the object. The target could be symbolic, an individual or an organisation but could also be a part of a critical SCADA system such as banking transactions, transmission links, traffic control systems and power networks et cetera.

Nunes [4] argues that there are three effects that may occur through information warfare and they are:

³ A pure peer-to-peer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network (Wikipedia)

⁴ Bit-torrent (= data swarming) is a file sharing technique (peer-to-peer communication protocol) providing faster downloading capability. BitTorrent is a method of distributing large amounts of data widely without the original distributor incurring the entire costs of hardware, hosting and bandwidth resources.

- **Physical effects:** physical destruction of information structure with the consequences that an operation cannot be fulfilled in a proper way because the information services could not be used fully (DOS-attacks⁵). A number of weapons and techniques could be used to knock out electronics; some of them are non-lethal EW weapons such as EMP⁶ and RF⁷.
- **Syntax effects:** the purpose is to attack the logic of the information system by delaying information and/or by developing “unpredictable” behaviours in information through, for instance, the introduction of viruses and trojans, and other hacking activities which include IT-weapons (CNO).
- **Semantic effects:** to destroy the trust in the system and information by manipulation, change of information and deception which may be harmful for the decision making process.

One conclusion is that there are a wide range of possible targets to attack and the effects and consequences regarding death-rates etc, vary. Regardless of whether the object is a symbol, physical infrastructure, an organisation or an individual, the antagonist may in some cases wish to achieve political-ideological-religious aims by his actions. In these cases the insurgent wants to draw attention and to show to the public that the government and other authorities have failed to provide safety for the citizens. A feeling of distrust may arise in ordinary people who may feel that the systems or the persons responsible for administrating them can't be trusted.

In other cases the insurgents don't want to be detected at all depending on their mission. That case is perhaps the most feared situation of all for authorities working with counter insurgency in the cyber arena.

⁵ DOS – Denial of Service

⁶ Electro Magnetic Pulse weapons

⁷ RF-Radio Frequency

The diagram below shows an example of *actor-target-effect chain* which summarises how an antagonist in different phases could plan and accomplish a cyber operation as well as the effects and consequences of the digital attack.

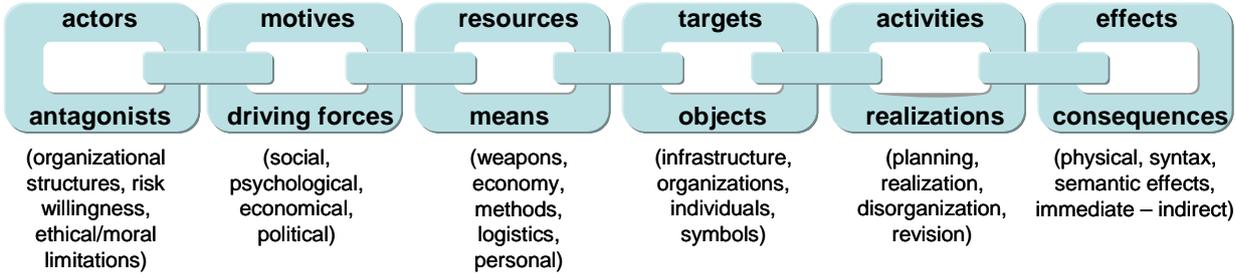


Figure 1. Actor-target-effect chain

2. Change of cyber terrorism modus operandi

Cyber terrorism is a development of traditional terrorism in a new arena using other means but with the same political and ideological aims. The advantages for cyber antagonists are the fact that modern society is heavily dependent on computer networks especially the Internet. The development of cyber terrorism can also be related to misjudgement by western intelligence authorities. To some extent have they failed to understand the insurgents’ resources, willingness and motives.

Cyber terrorists are very keen to find information that will help them to map critical infrastructures. Directed attacks against databases are a growing problem in order to collect sensitive information about specific targets, their structure and the level of information security. Another area of concern is the ongoing attempts to plant corrupt information into sensitive databases such as air traffic control systems, nuclear power systems and the pharmaceutical industry. These activities are well planned with clear purposes and goals for the operation as well as desired effects and consequences.

The cyber terrorist focuses mainly on civilian targets. Compared to military objects civilian targets are more vulnerable and less protected. Moreover, from an effect perspective the consequences for society will be bigger and it will probably also result in more media attention.

A trend since 2004 is both the change of target picture and modus operandi. The actors have gone from using quite simple working methods to being very rational and sophisticated with great accuracy in their actions. Historically, the cyber antagonists have based their methods on “fishing with a large net” in order to get viable information of any kind. Today their approaches have changed. If they want specific information they are using smaller and more granulated fishnets and only try to catch the fish they are after. Hence, the key questions

are: what types of methods are being used by the insurgents and for what purpose?

This chapter describes the development of this new professionalism exemplified by al-Qaeda and other terrorist groups such as al-Mujahedin and their usage of modern information technology techniques and procedures for ideological and political purposes.

2.1 The al-Qaeda example

In the early stages of the battle against terrorism, the western intelligence authorities misjudged al-Qaeda's strive to become an actor in the cyber arena. For a period of time some "experts" on terrorism thought that the organisation was more or less based on a bunch of misled individuals that lived under simple conditions in the Torabora-mountains in Afghanistan. Moreover, they were thought to lack overall strategies and goals others than traditional terrorism as well as the competence to use modern ICT⁸ techniques.

The problem with such narrow description is that it doesn't consider either the educational elite that is the basis and inner circle of the organisation nor the leadership and organisational structure. The terror group is built on decentralised networks with relatively autonomous cells spread over a large number of countries in all continents. There is no direct contact between the cells and top management acting as a central command. The development of an overall ideology, description of main objectives and initiator of attacks are defined by the top level. The autonomous groups plan and conduct operations by themselves.

A possible strategy and way of working in the preparation process for a cyber operation is the following:

Within strategic management so called "dispatchers" coordinate the information gathering process looking for suitable targets to be attacked. The reasons for using dispatchers are, except for the coordination process, to reduce own vulnerabilities and to limit the cyber terror networks knowledge of its own size and channels. If the counter insurgency authorities discover the network the damage will be limited. A member of a cyber network doesn't necessarily have to have any ideological or political sympathies. Moreover, people at lower levels do not always know that they are a part of an operation. Instead they are used as useful idiots for the inner circle's higher intents and purposes.

Through the dispatchers the top management level tries to attend actively on as many "bulletin boards" as possible on the Internet that discuss information

⁸ ICT – Information Communication Technologies

assurance, cracking and hacking techniques etc. The purpose is to create channels and to make contacts with hacker- and cracker communities on the Web. By using faked usernames and identities they can act anonymously and pretend to be “legal” members of the community. When a membership is established they try to get sensitive information from the bulletin boards by adding questions and “thoughts”, for instance regarding types of security problems a target system or network may have. The questions is said to describe problems that the (fake) member can’t solve by him self.

By using a method built on pieces of a puzzle, where questions are added in small portions to a number of bulletin boards, they can gather relevant information piece by piece. Over time a clear picture of the selected target system and its vulnerabilities is produced. Based on that information the critical infrastructure will be reviewed together with methods for making penetration attacks. This information is appropriated without displaying either the full purpose of the operation or those behind the questions.

Consequently, the task for the dispatchers is to co-ordinate and to synchronize contact people towards the hacker and cracker communities. Dispatchers may also organise the requested information and deliver it to the dispatchers contact at top level management.

In 2005 the London police found in a raid e-mail correspondence between the Islamic organisation *al-Muhajirun* highest ranking leader Omar Bakri Mohammed and well known al-Qaeda sympathizers. The documents included the following content:

"In a matter of time, you will see attacks on the stock market. I would not be surprised if tomorrow, I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."

According to Hamid Mir, editor at the newspaper Ausaf, Usama bin-Laden said following:

" that hundreds of young men have pledged to him that they were ready to die and that hundreds of Muslims scientists were with him and who would use their knowledge in chemistry, biology and ranging from computer to electronics against infidels".

Moreover, Bin-Laden is said to be given instructions to his sympathizers similar to “it is very important to attack the American economy because of the fact that US military strength is based on the economy”. The above mentioned quotations and statements describe quite well the capability of the al-Qaeda’s inner circle to judge what type of technological competence is required for conducting cyber attacks.

Recruitment

In comparison to the strategies and methods used by traditional terrorists in recruiting and converting young stray persons of Muslim background to become suicide bombers, the logic of cyber terrorism differs somewhat as does the work to develop competence and recruit the right people.

The vein of the terrorists is based on a good and continuous supply of sympathizers. There are several methods for recruiting self-sacrificing individuals. Common ways are articles, using local preachers, audio-videos and cd's describing the "cause". Other more intricate ones are recruitment sites on the Web. The websites describe the history of the organisation and overall goals of the struggle. These websites are often linked to other sites that could be of interest to a dedicated person and encourage enlistment.

The people they want to recruit for cyber actions are very skilled, often with higher education from universities. They understand the western culture and some of them are born in Europe and USA with full citizenship. Contrary to traditional terrorist, they are not potential suicide bombers.

The terror groups also use web pages that make it possible to donate funds for deserving purposes or operations that will be conducted. Some examples of interesting web sites are:

www.hamasonline.com

www.hizbolah.org

www.farcep.org/pagina_ingles

www.earthliberationfront.com

The e-mail correspondence and recruitment sites show that al-Qaeda and other insurgent organisations have moved from traditional terrorist activities into the cyber arena. The impression is that the opponent is well qualified with good ability to take action. The members have high education, good training and the organisation thus has access to competent individuals with knowledge of information technology.

2.2 Other examples of cyber terrorism

Another type of insurgent in the cyber arena is the terror group *al-Mujahedin*. The organization is, compared to al-Qaeda, based and sponsored by a single country in the Middle East.

In March 2007 an Islamic recruiting site was found with a directed request to the viewers to join a special pact called "Hilf al-Muhajaidin". The reader was informed that, in order to be enlisted, he or she must accept leadership of Muhajaidin brigades. The purpose, in translation from Arabic, was to

“conduct cyber warfare, to solemnly offer obedience to its leaders in all situations, not to question the leadership as well as not to hesitate to conduct attacks towards goals that violate or could harm Islam and Muslims”.

The request shows clearly that new forms of terrorism appear to be addressed solely to well educated persons and not to suicide bombers in a traditional sense. Furthermore, the supporters of the organisation perceive themselves as devoted soldiers closely united by a pact in order to execute an ideological mission. Today there are at least six prominent hacker groupings that represent Muhajaidin with their own websites.

Except for recruitment, the websites are used as communication links between other groupings that are involved in the electronic jihad. Some examples of information that is co-ordinated from the websites are: IP-addresses to the target that will be attacked as well as the type of information that will be transmitted and to whom. To avoid any discovery attempts from counter insurgency authorities, those responsible for the websites encourage and teach the supporters how to behave anonymously on the Internet.

During March 2007 an Islamic forum carried out a survey on the Internet directed to its Muslim “hactivist brothers”. The questions addressed to the respondents were to point out without any order of precedence the most important targets for an electronic jihad attack. The answers show that the hactivists prioritize websites associated with Western financial systems, homepages connected to CIA/FBI as well as servers used by the military. Only some weeks after the proposal on the forum, a list of IP-addresses to key western military institutions was published on one of the Islamic hacker grouping websites.

Simultaneously, another group declared in a web message that the group under the code name “the Electronic Guantanamo Raid” had well defined plans including dates to conduct cyber attacks against US banking systems. At the last moment the operation was cancelled due to a warning to the banks. The web message clarified also that:

” the panic shown by the intense media attention, points out that it is important for us to attack sensitive web pages”.

The messenger added following:

“if we attack websites serving financial exchange and banks, and we makes them inaccessible for days or only for couple of hours, that will render multi million damages”. “By that we proclaim to all members of this forum to focus on that type of websites. We invite all other Muslims that have the possibility to take part in the Islamic intifada, to attack website connected to American bank-and financial system”.

Furthermore, a suggestion was presented describing methods for the electronic jihads to conduct denial of service attacks, viruses etc, with the aim of shutting down vital nodes to create financial chaos. From a counter insurgency perspective, information on whether the jihadists have been successful or not in their intentions is vague and unclear. The information shown on jihad websites is limited with two exceptions.

The first example is from October 2006. In a message on an Islamic website a direct link was shown connected to surveillance system at Anchorage airport. There was also a link to an administrative system that gave the “surfer” access to the airport security cameras.

If this was an authentic penetration campaign, it indicates that Islamic hackers have pretty good computer capabilities due to the fact that the systems were guarded by intense security arrangements.

The second example is from 2005 when the 22 year old Londoner Younis Tsouli, better known as Irahbi 007, was taken into custody by the British police. In his short but vigorous existence as cyber terrorist he managed the hacker manuals of the Mujahedin members. Irhabi also penetrated American university servers and used them for loading up files with jihad related contents.

3. Conclusion

Terrorism in the cyber arena is a growing problem. In order to reduce danger to the open society from online threats as well as to act proactively, it is important to gain knowledge and to develop strategies and tactics for counter-action. The methods must be adapted to the change of insurgent logic and modus operandi. A fruitful method may be the actor-target-effect chain together with other procedures. Moreover, the threat from cyber terrorism will be a challenging task to deal with for the law enforcement agencies around the globe. Co-operation between authorities and organisations is therefore a necessity.

References

[1] Collin, B. (1997). *The future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*. 11th Annual International Symposium on Criminal Justice Issues. <http://afgen.com/terrorism1.htm>

[2] Heickerö, R., Hyberg, P., Olsson, G., Renhorn, I., Jonason, T., Eklöf, F. (2004). *Telekrig i breddad hotbild*. FOI-R 1370 Underlagsrapport

[3] Collin, B. (1997). *Ibid*

[4] Nunes, V. (1999). *The impact of New Technologies in Military Arena: Information Warfare*. Conference paper: International Congress of Military Press, Lisbon 13-16 September 1999.

Other references

[5] Giacomello, C. (2004) *Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism*. Studies in Conflict & Terrorism. University of Bologna, Italy. Taylor & Francis Group. ISSN: 1057-610X print/1521-0731 online

[6] Heickerö, R (2006). *Some thoughts on the application of military theory to Information Operations and Network Centric Warfare*. CCRTS Symposium, San Diego, USA. June 2006

[7] Heickerö, R. (2006). *Some aspects on cyber war faring in information arena and cognitive domain*. ICCRTS Symposium, Cambridge, UK. September 2006

[8] Heickerö, R (2006) *Informationskrig i cyberrymden. Elektronisk och digital krigföring i en breddad hotbild*. Underlagsrapport. FOI-R—2028--SE

[9] Parks, R., Duggan, P. (2001). *Principles of Cyber-warfare*. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United States Military Academy, West Point, NY, 5-6 June, 2001. ISBN 0-7803-9814-9

[10] Heickerö, R., Larsson D (2008). *Terror online. Cyberhot och informationskrigföring*. Conopsis Förlag. Stockholm. ISBN 978-91-633-1842-9

[11] Weimann, G. (2004). [WWW.Terror.Net: How terrorism uses the Internet](http://www.usip.org/pubs/specialreports/sr116pdf). United States Institute for Peace, special report number 116. www.usip.org/pubs/specialreports/sr116pdf.