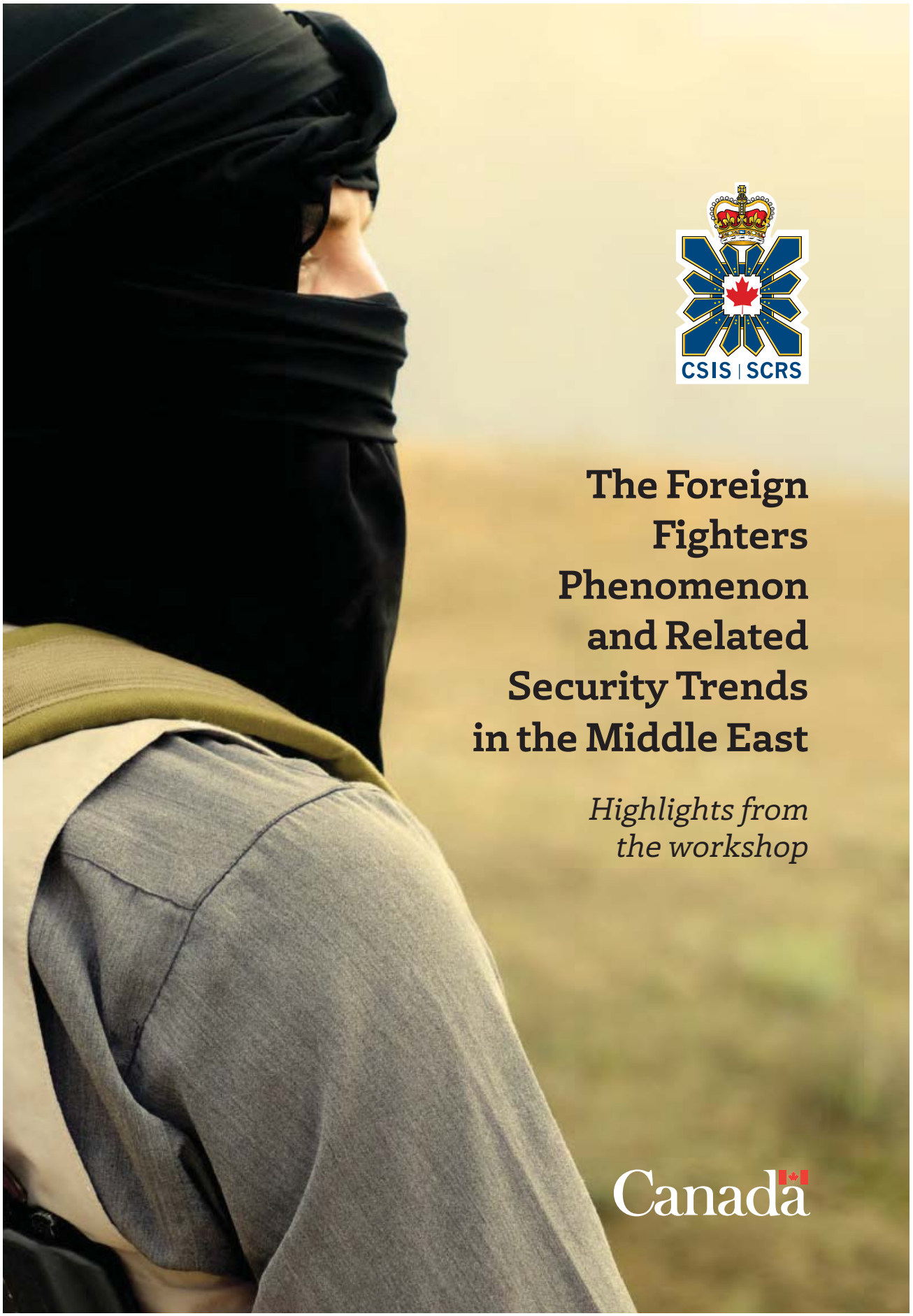

CSIS | SCRS

The Foreign Fighters Phenomenon and Related Security Trends in the Middle East

Highlights from the workshop

Canada

Think recycling

This document is printed with environmentally friendly ink

World Watch: Expert Notes series publication No. 2016-01-01

This report is based on the views expressed during, and short papers contributed by speakers at, a workshop organised by the Canadian Security Intelligence Service (CSIS) as part of the CSIS academic outreach program. Offered as a means to support ongoing discussion, the report does not constitute an analytical document, nor does it represent any formal position of the organisations involved. The workshop was conducted under the Chatham House rule; therefore, no attributions are made and the identity of speakers and participants is not disclosed.

www.csis-scrs.gc.ca

Published January 2016
Printed in Canada

Photo credit: istockphoto.com

The Foreign Fighters Phenomenon and Related Security Trends in the Middle East

Highlights from the workshop
28-29 October 2015

Table of Contents

The jihadist digital empowerment revolution

Chapter 3 – The jihadist digital empowerment revolution

In the past four years, Western countries have witnessed a veritable explosion in jihadist activity. By even the lowest estimates, more Western Muslims have gone to Syria than to all previous foreign fighter destinations combined. Polls, Internet activity and other anecdotal evidence suggest there is more support for the Islamic State in Iraq and the Levant (ISIL) today than there ever was for Al-Qaeda in the 2000s. The number of attack plots is only marginally up, but still at their highest level since 2001.

A root cause of this development is the unprecedented freedom of operation that jihadist activists have enjoyed on the Internet since around 2010. After a period in the late 2000s during which jihadists were struggling to communicate safely online, they now operate with relative impunity on a range of stable platforms. This helps foreign fighter recruitment considerably by exposing more people to propaganda, offering better information about the logistics of joining and facilitating the 'bridgehead effect', whereby early movers inspire friends at home.

Explaining the jihadist renaissance

The sudden increase in foreign fighting and ISIL support in the West in the early 2010s—the jihadist renaissance for short—is a formidable social scientific puzzle. It happened so quickly that it cannot be explained by socio-economic change among Western Muslims, be it poverty, marginalisation or identity problems. It also cannot be ascribed to changes in jihadist ideology, which has stayed broadly the same for many years. Something else must have changed.

Many have rightly pointed to the sudden eruption of the Syrian war, whose features—its many civilian deaths, proximity to Europe or place in the Islamic apocalyptic tradition—made it a particularly attractive destination. Others have stressed the sudden lowering of constraints on foreign fighting, arguing that international support for the Syrian opposition and weak policing of the Syrian-Turkish border in the early years made Syria much easier to reach than other theatres of conflict. Yet others attribute the increase to ISIL's

propaganda efforts; ISIL is said to run a particularly sophisticated distribution apparatus and to produce particularly slick or impactful content.

All of these factors are probably important. Missing from the discussion, however, has been the dramatic change in the ability of activists to use the Internet for recruitment purposes. What is new today is not that jihadist use the Internet—they always did—but that they do so with greater ease and impunity than at any point in history. This 'digital empowerment revolution' coincided in time with the jihadist renaissance and has been a driver behind it.

Why it was not always this way

To appreciate the novelty of the situation, we must remind ourselves that seamless terrorist exploitation of the Internet is by no means a given. High-risk activists normally face two fundamental problems online: security and trust. To ensure that they do not get caught, hunted men must make sure that they are not tracked or monitored and that the people they interact with online are not spies. Security is hard to achieve because activists have incomplete information about the technology they are using. Trust is difficult to establish because of the so-called bandwidth problem (the absence of non-verbal communication cues, which makes it much easier to pretend being someone else). The more sensitive the communication exchange, the more acute the problems. Unilateral recruitment calls ("come to Syria everyone!") and general ideological chats ("I hate America"—"so do I") are not very sensitive because they are not illegal. Recruitment exchanges ("let's meet so I can introduce you to the brothers") and operational coordination ("you kill the guard and I lob the grenade") are much riskier to conduct online.

The extent to which terrorists experience trust and security problems is a function of technology and repression. New technologies can provide stealth or facilitate vetting. Weak online policing reduces the risk of getting caught. Because technologies come in bursts, we have historically seen a cat-and-mouse game between rebels and governments. When a new technology is introduced, rebels are digitally empowered for a while until governments catch up and roll back the rebels' gains.

The online operational freedom enjoyed by jihadist has therefore varied over time. A recent study documents a major shift in the sense of security and trust among online jihadist in the mid-2000s[61]. In the early 2000s, jihadist exploited digital technologies with relative ease. There were stable jihadist web sites, often registered under real names and sometimes displaying real contact details. In jihadist discussion forums, people felt secure enough to volunteer personal information that could reveal their location and identity, and counter-surveillance was not a major conversation topic. By the late 2000s, virtually all the static web sites were gone. In the forums reigned an atmosphere of paranoia; nobody revealed sensitive information, there were numerous posts about how to avoid surveillance, and rumours about infiltrators and honey-pot sites proliferated. It was rare to see specific information about how to link up with a militant group, and there was very little evidence of online recruitment transactions (in the sense of recruiter and recruit meeting first online and only after in real life). What had happened was that governments had realised around 2003-2004 that the web had become a safe haven and increased repression in the form of site take-downs, content monitoring, SIGINT collection, honey-pot sites and online undercover operations.

An unprecedented situation

Fast-forward to 2015. The static web sites are back again, more numerous than ever. Wordpress and Tumblr host hundreds of jihadist blogs, many of which offer specific advice about how to get to Syria. The forums are largely gone, but they have been replaced by Twitter and Facebook, where people regularly volunteer information (such as their location or photographs of their surroundings) that could in theory lead to their capture. On Facebook, especially, many write under their real names or poorly disguised pseudonyms, and everybody reveals their social network through their friends list. A plethora of apps such as Whatsapp and Kik allow for bilateral or small-group communication and are, by all accounts, being used for sensitive information exchanges. There is plenty of evidence of Internet-mediated recruitment exchanges. Compared with the late 2000s, online jihadists seem to have very few concerns about security or trust. It is only among active members of ISIL—the most at-risk subset of jihadists—that we see widespread interest in security-related advice.

It is not just the ability to exchange sensitive information that has increased. There has also been a quantum leap in the ability to project propaganda. In the past, viewing a jihadist video, for example, was a cumbersome process. You had to access a jihadist forum, locate the post, find a working download link (among the list of 20 to 50 displayed for redundancy), and then download from one of the file-sharing sites such as Megaupload (which were also used to distribute pirated music and porn). Today you just click a Youtube link or watch the video directly on one of the static sites such as Archive.org, Ansar Khilafa, or (until recently) Isdarat. Videos now also have much longer online lives, and they are all searchable, which they were generally not in the past.

Moreover, the availability of jihadist propaganda on mainstream sites like Youtube and Twitter has all but eliminated self-selection as a barrier to exposure. In the past, only people who actively sought out jihadist forums—ie, those who had already started a process of radicalisation—got to see jihadist propaganda. Today, YouTube may suggest a jihadist video for you in the right-hand column even if you search for something else, like “nashid” or “Badr”. Twitter and Facebook will suggest friends for you, potentially bringing you into contact with radicals two degrees removed. Once you are connected to a jihadist sympathiser on Twitter, an ocean of jihadist propaganda is just a few clicks away.

Generally we have a situation where it has never been easier for jihadists to communicate among themselves and reach potential recruits. Activists are doing things online today that would almost certainly have had them arrested in the late 2000s. Governments have basically lost control over the jihadist Internet. How did this happen?

Causes

The first reason is technology. The late 2000s saw the rise of new communication platforms that were better designed for online social interaction and the exchange of audiovisual content than previous platforms, hence their name: social media. Some of them reached a scale that allowed for exceptionally wide distribution. Others were designed to allow for more limited audience, but more secure communication. Some of the platforms, such as Facebook, also have a design that reduces the trust problem, because it displays more complex information about the user and allows for

the accumulation of user information (ie, the building of reputations) over time. Not only did we get qualitatively different platforms, we also got *more* of them, which has probably stretched surveillance resources.

A second reason is that the new platforms were owned by large Western corporations. Jihadists paradoxically came to enjoy more stability and protection on social media than on the open Internet, even though the platforms were US-owned. The forums of the 2000s could be taken down, hacked, taken over or mimicked. The US National Security Agency cannot do the same to Twitter or Facebook for obvious legal reasons. The policing of these platforms—which are effectively small internets inside the Internet—was thus left to a *private* police force, namely, the companies themselves. The companies, however, have different incentives and skill sets than a regular intelligence service and have, despite their good intentions, manifestly failed to stem terrorist exploitation of their services.

A third factor is safe havens. In the early 2010s, for reasons linked to the Arab Spring, several jihadist groups established territorial safe havens, especially in Syria and Iraq, but also in Yemen, Libya and elsewhere. Thus in any digital communication between a jihadist group and a supporter in the West, one side would be out of reach. Unlike militants in late 2000s Waziristan, who had to limit Internet use in the field for fear of being droned, jihadist in Syria could communicate with the outside world at a much lower risk of harm.

A fourth factor has been the resource constraint on intelligence services. The three previous factors would not necessarily have produced a digital free-zone if the new challenges had been met with adequate policing. Instead, Western intelligence services were left to deal with a much larger problem with roughly the same resources. As a result, the interaction effect of the digital empowerment revolution and political developments left security services overwhelmed. The Syrian war created more candidate foreign fighters, who exploited the new technological opportunities and quickly became so many that governments could no longer police online jihadism as before. A new equilibrium emerged in which security services had to focus on the most acute security threats, leaving minor infractions (such as running a foreign fighter

blog) alone. In this new normal, the threshold for what will land an online jihadist into trouble is much higher than it was in the 2000s.

Effects

The effects of the digital empowerment revolution for jihadist recruitment are fairly intuitive. Let us examine the main ones to highlight the mechanisms involved.

First is the exposure effect, which is that jihadist today are able to expose a much larger population to their propaganda than was the case in the past. The scale and design of the new platforms, the elimination of the self-selection barrier and the general media coverage of groups like ISIL combine to make it almost impossible for a young Muslim *not* to see jihadist propaganda at some point in their adolescence. Of course, propaganda exposure alone is rarely enough to trigger radicalisation, but it helps.

Second is the information effect, which is that prospective recruits now have much better information about how to join than they had in the past. In the 2000s, there were no blogs that told you how to get to Waziristan, what to bring, what to look out for, or what to expect. Today you can easily find extremely detailed travel advice for Syria. This not only enables, it also helps to motivate, because it reduces uncertainty about the risks ahead.

Third is the bridgehead effect, by which early movers motivate their friends at home to join them by reporting what it is like in the field. This can take the form of private messages (sms, pictures, short videos), semi-private messages (Facebook and Instagram posts, Whatsapp messages, etc.), and open messages (blog posts, pictures, videos). This type of home reporting occurred in the 2000s as well, but on a much smaller scale than today. If you are on the fence with regard to joining, seeing a friend—or simply someone who looks and talks like you—join before you and do fine can tip the balance. This is the single most important recruitment mechanism for Western foreign fighters.

A fourth potential effect is that militants start using the web more systematically for operational coordination. This a much desired capability for any terrorist group—the Holy Grail of tactical advancements—because it reduces the need to meet physically and increases the ability to strike at long distances. However, it

requires very high levels of confidence in the technology and trust in your interlocutors, so it is relatively rare. If the current trend towards online lawlessness continues, we will see more and more operational coordination over digital platforms.

Conclusion

A fundamental driver behind the dramatic rise in jihadism in the past five years has been the opening up of a digital sphere where militants can operate with relative impunity. Contrary to popular perceptions, this situation is new and avoidable.

If governments want to stem radicalisation, they can and must do more to police the jihadist Internet. There is a need for an immediate, large-scale, multinational effort to take the Internet back from the jihadists. Such an effort will necessarily involve a multitude of measures, but one could start with low-hanging fruits such as taking down static web sites and blogs. Then one must work with social media companies to police their platforms better. Security services could use tried-and-tested methods such as infiltration and information operations to undermine interpersonal trust among jihadists online. Some challenges, such as encryption, are of a technical nature and cannot be solved by decree, but many others are a matter of political will and funding.

> *There is a need for an immediate, large-scale, multinational effort to take the Internet back from the jihadists.*

Of course, this is sensitive political territory, for everybody wants online privacy and nobody wants a thought police. There needs to be an open and informed debate about the premises for any such digital counter-offensive.

There are at least three reasonable arguments in favour or more online policing. The first is that much of what is going on online is already illegal, so for these phenomena we are only talking about enforcing existing laws. Second, there is arguably a difference between free speech and broadcasting. Few would argue that it is a human right to get air time on television to voice one's opinions. Why should it be on Twitter? Third, we are not talking about a

digital military coup, but a return to the situation of about 2010. It is not the policing that is new, but the lack of it.

Such a debate would benefit greatly from more openness on the part of the security services. Many citizens are opposed to online policing because they do not know the extent and nature of the problem. Security services should provide the public with detailed, real-life examples of the challenges they are facing.

Social media are but the latest in a series of technology shocks over the past twenty years which have helped temporarily subversive non-state actors communicate. In the past, governments caught up with online rebels and re-established a degree of authority. We must do the same again, or jihadism will continue to grow.