الجامعة البريطانية في دبي

The
British University
in Dubai

21^{st} Century Warfare: How Information Technology Has Fundamentally Changed Global Warfare - An Analysis of Insurgencies' Use of IT

حرب القرن الحادي والعشرين: كيف غيّرت التكنولوجيا الحرب العالمية
دراسة حالات التمرد واستخدام تكنولوجيا المعلومات

by

MOHAMMAD NADER MOHAMMAD ABDULLAH FIKRI

Dissertation submitted in fulfilment
of the requirements for the degree of
MSc INFORMATION TECHNOLOGY MANAGEMENT
at
The British University in Dubai

November 2018

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

The author whose copyright is declared on the title page of the work has granted the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author’s express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

Abstract

Methodology

This paper utilizes a qualitative approach to provide a case study analysis of the rising use of technology by insurgents. Examining the literature and making a comparative analysis of the trends of recent years allowed the researcher to come to the conclusion of the rising necessity of cybersecurity in contemporary warfare. A quantitative approach in such a case would have been limited due to the lack of reliable statistics available as well as the more sterile nature of results it would provide.

The 21st century has seen a change in the type of warfare waged globally. Whereas the 20th century was characterized by decolonization and states warring against one another, the 21st century has witnessed a shift in global warfare where non-state actors such as radical groups are gaining momentum and causing significant mayhem. The accessibility of radical groups to wage war on a global level has been exacerbated in recent years by the widespread usage of information technology on an individual level and the resulting compression of time and space.

Both these factors, the rise of non-state actors and the usage of information technology, has disrupted the way global warfare is waged. This dissertation focuses on examining the ways in which global security in the 21st century has changed due to insurgents' access to information technology. By focusing heavily on the available literature and findings conducted of the insurgents in Iraq and Syria, this research aims to provide recommendations on the ways in which governments must now reassess their security needs by taking into account the changes in 21st century information technology.

Information technology is a double-edged sword; the abuse of it by the wrong hands can cause global chaos, however, it is also a fundamentally important tool in the counterterrorism effort as well. As technology continues to advance and as social networks and IT equipment become more

accessible to individuals, a major portion of global antiterrorism efforts will shift to the digital sphere.

After reviewing the findings from literature and references of insurgents’ usage of IT, it became clear that social media was a catalyst for the rapid spread of their ideology and propaganda. Social media networks were used both to brainwash the public and recruit new members. Government websites and databases were hacked by cyberattacks and sensitive information made public. These findings from the literature review conducted; demonstrated that they had a well-developed, deeply-strategized IT and media strategy and that when they emerged globally seemingly overnight, the world was taken aback and governments were unprepared with how to deal with their digital prowess. This has brought to light the importance of a globally concerted effort to give cyberterrorism the importance it deserves in counterterrorism efforts.

نبذة مختصرة

لقد شهد القرن الحادي والعشرين تغيراً في نوع الحرب التي يتم شنها على مستوى العالم. في حين كان القرن العشرين يتميز بإنهاء الاستعمار والدول المتحاربة ضد بعضها البعض ، فقد شهد القرن الحادي والعشرين تحولا في الحرب العالمية حيث يكتسب الفاعلون من غير الدول مثل الجماعات المتطرفة زخما ويسبب لهم فوضى كبيرة. لقد تفاقمت إمكانية وصول الجماعات المتطرفة لشن الحرب على المستوى العالمي في السنوات الأخيرة بسبب الاستخدام الواسع النطاق لتكنولوجيا المعلومات على المستوى الفردي والضغط الناتج عن الوقت والمكان كل هذه العوامل ، صعود الجهات الفاعلة من غير الدول واستخدام تكنولوجيا المعلومات ، عطلت طريقة شن الحرب العالمية. تركز هذه الرسالة على تحليل الطرق التي أثرت بها تكنولوجيا المعلومات في أيدي المتطرفين في الأمن العالمي.

إلى توضيح الطرق التي يجب على الحكومات الآن من خلالها معالجة احتياجاتهم الأمنية من خلال مراعاة ضعفهم بسبب تكنولوجيا المعلومات .تكنولوجيا المعلومات هي سيف ذو حدين. إن إساءة استخدامها من قبل الأيدي الخطأ يمكن أن تسبب فوضى عالمية ، ومع ذلك ، فهي أيضًا أداة مهمة بشكل أساسي في جهود مكافحة الإرهاب أيضًا. مع استمرار التقدم التكنولوجي ومع زيادة إمكانية وصول الأفراد إلى الشبكات الاجتماعية ومعدات تكنولوجيا المعلومات ، سيتحول جزء كبير من جهود مكافحة الإرهاب العالمية إلى المجال الرقمي .من خلال فحص استخدام المتمردين لتكنولوجيا المعلومات ، أصبح من الواضح أن وسائل التواصل الاجتماعي كانت بمثابة حافز للانتشار السريع لإيديولوجية ودعوتهم. تم استخدام شبكات التواصل الاجتماعي لغسل دماغ الجمهور وتوظيف أعضاء جدد. تم إختراق المواقع الإلكترونية وقواعد البيانات الحكومية من خلال الهجمات الإلكترونية والمعلومات العامة التي تم نشرها. أظهرت حالة المتمردين أنهم يمتلكون استراتيجية تكنولوجيا معلومات ووسائط متطورة ومتطورة بشكل جيد ، وأنه عندما ظهروا عالميًا بين عشية وضحاها بين عشية وضحاها ، كان العالم متفاجئًا وكانت الحكومات غير مستعدة لكيفية التعامل مع براعتهم الرقمية. وقد أوضح هذا أهمية بذل جهد متضافر عالميًا لإعطاء الإرهاب السيبراني الأهمية التي يستحقها في جهود مكافحة الإرهاب.

Acknowledgement

I would like to thank my workplace, Telecommunications Regulatory Authority, by believing in me and making my master’s degree possible thanks to their generous scholarship.

I would also like to thank the faculty of BUiD and especially my advisor Professor Cornelius Ncube for his valuable insight and advice into the path this dissertation ultimately took.

Last but not least, I would like to express my gratitude to my family who has provided me with unwavering moral support during this time as I wrote my dissertation while completing my military national service duty.

Table of Contents

List of Illustrations and Tables

Chapter 1: Introduction

The 21st century has seen the global disruption of traditional modes of defence and security. The rapid growth of information technology that has caused a widespread shrinking of the paradigms of space and time has left no stone unturned. The effects of the IT revolution are most notably felt in the sphere of international relations, with technology changing the way wars are waged and affecting the vulnerability of states and subsequently how these states protect themselves.

The world order has always been dominated by opposing ideologies of realism and liberalism, and each ideology has a different conception of the effect of IT in traditional state security. Regardless of which ideological camp one belongs to, it is hard to deny that changes in global warfare that have been brought about by cyberterrorism, a by-product of the IT revolution.

This paper argues that cyberterrorism has fundamentally changed the way a state perceives its security and the way global warfare is waged. By using a case study of insurgents, I further demonstrate using concrete examples the shift in the global balance of power and the immediate need for states to readdress their current security framework to include an approach that focuses heavily on cyber threats.

This dissertation begins with a literature review encompassing the traditional ideological frameworks of realism, liberalism and constructivism, as well as a critique of current research in the field of cyberterrorism. It then progresses to arguing how IT is disrupting traditional methods of security by demonstrating the changes caused by cyberterrorism. Next, this paper focuses on a desktop research of the viable sources of study of insurgents to further back up its claims. The research review is the core of the dissertation where insurgents' social media prowess is examined as well as their usage of cyberattacks to further their agenda.

Finally, the paper finishes with a review of what is currently being done to combat cyberterrorism and provides recommendations of what more could be in the coming years.

Literature review

Theoretical Review

There have historically always been two opposing parties when it comes to the ideologies of politics. On the one hand are the realists, and this is where right-wing politics originally stems from. On the other hand, is liberalism, which planted the seeds for left-wing politics. In recent decades, however, there has also been the rise of constructivism, a third political ideology which was developed in response to the rapidly changing political and economic environments of the 20th century. This paper takes a constructivist point of view to argue its points.

Realism

To begin with, realism is the perhaps the oldest school of political thought. Greek philosophers such as Thucydides (writing on the Peloponnesian war) and Thomas Hobbes argued that states are essentially motivated by self-interest and thus exercise their power in an effort to demonstrate their own abilities and to curb the power-gaining tactics of other countries (Goldstein and Pevehouse 2012). For realists, politics are power politics and states must rely on themselves and no one else for help. They believe that the international system (the global environment where nations and states interact) is constantly in a state of anarchy, and as such, each state must look out for themselves. Thus is played out the oldest game in international relations, that of the balance of power (Nye 2010).

In realism, states are considered the most important actors in international relations (Goldstein and Pevehouse 2012) and the need for a heavily fortified state through spending heavily on the military is considered paramount. Major thinkers in the realist school of thought, such as Carl von Clausewitz, discuss the importance of military strategy and tactics by stating that the "maintenance of military force is always a necessary condition" (von Clausewitz 1832).

Liberalism

In liberalism, proponents take a different view on global power politics. They see states as inherently cooperative and they believe in the importance of international organizations in global governance. Liberals believe that states can work together to overcome mutual problems and they do not see the international system as one of a constant struggle and balance of power (Goldstein and Pevehouse 2012). Instead, they see positivity and the inherent good nature of states.

Constructivism

This paper identifies with the ideological merits of constructivism. Constructivism does not propagate the rigid ideas of realism, nor does it always see states as inherently good. Constructivism believes in the fluidity of the international system and the subsequent shifting national interests of countries. Constructivism believes that state's behaviors are governed by regulative and constitutive norms which are basic rules influenced by current political scenarios. Using constructivism as a theoretical framework allows us to understand states' behaviours as ones that change through time based on shifting national interests and the change in global power politics and the way war is waged (Goldstein and Pevehouse 2012; Nye 2010).

Insurgents Literature Review

In conducting a case study on insurgents' methods of cyberterrorism it became clear that this type of terrorism could be divided into two parts. The first is the usage of digital social networks by insurgents to a) recruit members and b) spread propaganda. The second is cyberattacks conducted by insurgents which range from online financial theft to defacing government websites. The former had plenty of resources available for study. However, there was comparatively a great dearth in resources for the latter. Based on my research I have tried to understand why such a disparity might exist and I believe that much of it has to do with government security and privacy. Firstly, governments will always try to play down any cyberattacks conducted against them as that would mean they are vulnerable. These attacks are often downplayed and for the sake of the government's own security, largely ignored when it comes to the general public audience. Additionally, it is definite that many studies and researches are conducted into these attacks but that they are conducted by the governments themselves, and that the documents are thus kept private and classified. If such information detailing how a cyberattack was made possible were free to fall into anyone's hands, the government's vulnerability will increase as potential cyber radicals would be able to better understand how these attacks were conducted. After careful examination and extensive research in the field of national security on the digital, I can confirm that the privacy of such classified documents are of the utmost importance in order to protect and reduce vulnerability. However, the need for governments to coordinate and work together on the combating cyberattacks is as necessary as their need to work together on physical military offenses.

Scholars and researchers such as Charlie Winter, J. M. Berger, A. Zelin and others have published numerous quantitative and qualitative studies detailing insurgents' usage of social media. Many of these researches, such Zelin's 2015 analysis of content output by insurgents over a period of a few months, or Berger's analysis of Twitter logs, or Charlie Winter's work examining the content of insurgents' digital magazine focuses on how insurgents use information technology to propagate information and recruit members. However, as previously mentioned, there was comparatively a huge lack of studies in the field of cyberattacks conducted by insurgents. It would be interesting to examine in a more in-depth way the strategies used in insurgents cyberattacks and the ramifications of these attacks, however, that is beyond the scope of this dissertation.

Chapter 2: DISRUPTION OF TRADITIONAL METHODS OF SECURITY

The spread of technology and the ease of access to it by individuals has caused a deep shift in the way war is waged. Many non-state actors such as guerrillas and radical organizations have shifted their efforts to the cyber world. There are several reasons as to why this shift has taken place. Firstly, and perhaps most importantly, was the relative anonymity of the online world (Burke 2016; Conway 2017). It is hard to track down a user when the right techniques and encryption are applied. Secondly, it was extremely economical. Conducting cyberattacks needs hardly any capital compared to waging an actual, physical combat that requires mobilization, equipment and logistical planning (Carter et al 2014). Third, the internet is easy, effective, and quick (Winter 2015). These three qualities soon attracted radicals and caused a shift in the way global warfare is conducted.

The fundamental shift in the way war conducts itself can be traced back to the wave of decolonization that took place in the 20th century after the two world wars. After the resource-draining wars, European powers (who were previously the major powers in the world) found that they could no longer sustain their sovereignty over disparate and remote areas of the world in Asia, South American and Africa. This was coupled with resistance movements on the colonized lands that had been growing in momentum since the late 19th century. Combined, these two forces led to the breakdown of colonization and the establishment of new states (Goldstein and Pevehouse 2012; Nye 2010). This is where many of the world's current problems began. The European powers who implemented the technicalities of the decolonization movement paid little attention to the cultural sensitivities of the new countries they were creating. Borders were arbitrarily drawn and soon, ethnic groups who were historically major enemies found themselves lumped together in the same country. Conversely, ethnic groups were split between two countries on opposite sides of a border. These led to grievances and ethnic conflict which is what characterized the wars of the 20th and 21st centuries. “This is a major source of conflict as there is a mismatch between perceived nations and actual state borders” (Goldstein and Pevehouse 2012).

A second major force to disrupt the traditional methods of war and security was the information technology revolution (Goldstein and Pevehouse 2012). This revolution has affected both state actors and non-state actors in fundamental ways and has forever changed perceptions of security.

Thus, since the 20th century two major changes have taken place in the international system. The first is the growing emergence of non-state actors in international politics and the second is the increasing use of information technology by both state and non-state actors to further their means.

“Global telecommunications are profoundly changing how information and culture function in international relations” (Goldstein and Pevehouse 2012). Information technology in international relations is a double-edged sword; not only does it enable countries to more effectively manage their populations, it also provides non-state actors with powerful tools to conduct opposition movements (Goldstein and Pevehouse 2012). The effects of the latter override the benefits of the former. “Information affects power and governments of all kinds will find their control eroding during the 21st century as IT gradually spreads and costs continue to decrease (Nye 2010).

Non-state actors such as radical movements are finding it easier to operate than ever before due to information technology. They use cell-phones and the internet to raise money and recruit members. Technology is enabling them to use powers that were once only in the domain of states and their respective governments (Nye 2010). Thus is born a new form of terrorism; cyberterrorism.

A relatively new term in international relations terminology, the definition of cyberterrorism and the legal eventualities it entails is not universally agreed upon. For the sake of clarity, this paper adopts the following definition for cyberterrorism that I have created after extensive research:

> *Malignant acts performed by radical groups either by using information technology as a means* [i.e. to recruit or gather funds], *or as the main method to conduct attacks* [i.e. hacks and cyberattacks].

There are several reasons why information technology has been appropriated by radical organizations. Firstly, IT provides "cheap and quick communication" (Veerasamy and Grobler 2011). This aids in not only recruiting members but also in conducting attacks faster as social apps such as WhatsApp and Viber make it easier to coordinate logistics.

Secondly, proficiency in information technology and particularly cybercrime enables radical organizations to acquire large amounts of capital through hacking, thus giving them the ability to fund themselves (Veerasamy and Grobler 2011). Previously, radicals had to gather funding through extensive fundraising efforts by attracting sympathizers; now, they can gather funds independently through hacking.

Thirdly, the internet provides an ample arena for radicals to spread their ideology. "The web turned out to be the perfect arena for radical groups as it offered easy access, little or no regulation, and anonymity" (Mediterraneanaffairs.com). Terrorists use websites to spread their propaganda and also to provide instruction to new recruits. The condensation of time and space due to the information technology revolution has proved to be the biggest catalyst for the spread in radical activities.

Anti-Forensics Activities

It is fairly easy for radicals trained in hacking to cover their steps. Veerasamy and Grobler (2011) state that radicals currently engage mostly in these anti-forensics activities:

1. Dead Dropping
2. Steganography
3. Encryption
4. Proxies
5. Anonymising
6. Cloaking trends

Additionally, radicals often deface websites to "demonstrate their capability and create fear" (Veerasamy and Grobler).

As we can see, the realist ideology is no longer effective in combating the unique security challenges of the 21st century. Firstly, realism states that the major security dilemmas of the international system have to do with states alone. As we have seen, non-state actors such as radical groups are challenging current security frameworks to refute this claim. Very rarely are wars now conducted between two sovereign governments. Secondly, realists' traditional focus on heavily investing in military fortification is also undermined due to the permeating nature of information technology and the security challenges it posits.

Chapter 3: Case Study Analysis: Insurgents

Insurgents is the first radical organization to rely heavily on social media networks to recruit new members. According to Sheetz (2016), the following applications are the most heavily used among members and sympathizers of the insurgents: “Telegram, Threema, Kik, Wickr, SureSpot and Whatsapp". It is clear to see that the applications receiving the highest usage are those that promote instant communication. What is unique about the global battle against insurgents is that even though military forces are managing to take back cities and quash insurgents’ physical ‘caliphate’, the ‘cyber caliphate’ is very much alive and well and has the ability to constantly resurface (Winter 2017). This cyber caliphate is what is causing the perpetuity of insurgents and global governments are still not redirecting their efforts to combat insurgents on the digital plane (Governmenttechnology.com, mediterraneanaffairs.com).

Upon reading the insurgents’ “Media Operative”, one can clearly see insurgents’ understanding of the strong capabilities of the media in propagating its message.

This section is divided into two parts. In the first part, I will study the use of social networks by insurgents to recruit members and spread propaganda. In the second section, I will provide an overview of the cybercrime attacks committed by insurgents.

3.1 Insurgents, the Media and Social Networks

What struck people the world over about insurgents was the fact that many of its recruits were new converts to Islam. Many of them were Western men from regular middle-class backgrounds who had no links to extremism of any sort (Berger 2015; Awan 2017). How did these men get lured to insurgents in the first place? What were the means used to communicate? This section sets out to provide answers to both these questions.

In the first part of this section, we will discuss the usage of social media networks and the internet by insurgents. In the second part of this section, we will examine the cyberattacks created by insurgents. In both sections, we will provide an overview of the current literature and make a note of the potential opportunities for further study.

3.2 The usage of media and technology

Insurgents is the first radical group to fully capitalize on the opportunities provided by information technology and social media. They believe in the importance of information technology to the extent that they had a Minister of Information Technology, the late Abu Muhammad al Furqan (Berger 2015).

Charlie Winter (2017) of the International Center for the Study of Radicalisation states that insurgents believe the media to be a "powerful psychological weapon" and that in many cases they believe its potency can even "substitute…military and radical operations". According to the insurgents' media operative, "If launched effectively, media weapons [can] actually be more potent than atomic bombs…", and that "media jihad has far reaching potential to change the balance in respect to the war between the Muslims and their enemies" (Winter 2017). This itself is extremely indicative of the resulting challenges faced by global counterterrorism efforts. While insurgents were busy developing a detailed media strategy, global powers were still not giving information technology the importance it deserved. Thus, the world was taken by surprise by insurgents' ruthless and subsequently effective utilization of information technology and the media. Therefore, when counterterrorism efforts against insurgents began, the world had already fallen behind and was already at a disadvantage digitally. The impact of this is huge and cannot be downplayed. insurgents' utilization of information technology was intrinsic to its success not only in conducting its attacks but in its soft power ability of brainwashing and recruiting members.

The International Centre for the Study of Radicalization (ICSR) in London, UK has conducted some pioneering research on the field of insurgents and media. Charlie Winter (2017), one of ICSR's specialists in insurgents and terrorism has reiterated this point of insurgents' global advantage by the usage of its media by stating that:

"media weapons are calibrated with a view to attacking disengaged publics as much as they are geared towards hitting engaged militaries. This form of turbocharged, narrative-led terrorism- in which the insurgents' propaganda response to operations carried out in its name can be more impactful than the attacks themselves- has emerged as the foremost component of its asymmetric arsenal." (Winter 2017).

Like any political or radical group who seeks to gain power through brainwashing and scapegoating a particular segment of society, propaganda is extremely important to insurgents. In order to maximize their propaganda efforts, they have fully utilized social media and the internet. Not only do they use "conventional devices for propaganda like video releases, audio bulletins, and written materials" (C. Winter, 2017), but also social media networks.

The main aim of their propaganda strategy was to recruit members to their 'cause'. The way they did this was by exploiting social media networks in a way that included potential recruits and existing recruits as stakeholders in the process (Awan 2017; Badawy and Ferrara 2017). Apart from having 'official propaganda channels' on various social networking platforms like Twitter and Telegram, insurgents had a document titled the 'Media Operative' which they would regularly update and revise and republish. This document functioned like a handbook for insurgents' recruits and its subtitle was 'You are a Mujahid, too'. This document set out to recruit members to insurgents by making them stakeholders in the process. By developing this sense of fraternity and inclusion, they were able to recruit members from all corners of the world. People all over the world were surprised at insurgents' ability to recruit members such as young adolescent Western males who had no previous connection to Islamic or the Arabic-speaking world.

Insurgents' usage of social media networks and this operative which seemingly provided a sense of ownership to new recruits helped in this ability to attract people from far and wide. A sentence from insurgents' Media Operative document is indicative of their focus on including recruits as stakeholders:

"Everyone that participates in the production and delivery of propaganda should be regarded as one of the insurgents 'media mujahidin'. Furthermore, they assert that 'we are in a battle and more than half this battle is taking place in the battlefield of the media.'

As the first radical group to fully manipulate social media and information technology, global powers were at a loss how to respond.

3.3 The exploitation of social networks

As mentioned in the previous subsection, insurgents' successful manipulation of social media networks led to its ability to recruit members from all over the world and to spread its propaganda. In the previous section, we focused on the importance given by insurgents to media and information technology. In this section, we will take a closer look at how they exploited these social networks.

According to Alfifi and Morstatter (2018), social media gave insurgents to come directly in contact with the people they were targeting to recruit. The attraction of social media was its lack of editorial oversight and lack of rules. It became a "relatively lawless federated system" (Diresta 2018).

Previously, radical groups would communicate online using heavily encrypted methods. They would use password protected forums and they would mainly communicate in Arabic. What insurgents did differently was that it boldly used social media the way it was meant to be used. They took advantage of the freedom of speech made possible by social media networks and they used their 'branding' of their logo and slogans on all their platforms. Thus, they were the first radical group to use social media in the way it was intended to be used- albeit for ill-intentioned means (Conway 2017; Alfifi et al 2018). They also used the media to *appear* more active than they really were.

3.4 Recruiting members

The reason insurgents have been so successful in recruiting members is two-fold. First is its ability to effectively use social media as a means. Second, is their recognition of the need to constantly change and adapt. These two go hand-in-hand to explain insurgents' success at recruiting new members.

One way that helped the insurgents succeed in recruiting members online was its ability to segment their target audience (Zelin 2015). The content they would publish offline differed greatly from the content they would publish online. Not only did the type of content differ (as will be further detailed in the following section), but they also used several languages to target a potential international audience online, as opposed to solely Arabic for their offline content in Iraq and Syria.

This 'ability to manipulate their global consumers…[hobbled] counter-extremism policymaking.' (ICSR, 2018). insurgents are so detailed in how they craft their propaganda messages that each message not only has a target audience in mind, but also primary and secondary consumers (ICSR, 2018).

Charlie Winter (2017) in his ICSR report titled "Media Jihad: The insurgents Doctrine for Information Warfare" states that:

"[insurgents'] aggressive approach to outreach caught the world off-guard, …. The communications, tailored as they were for swift…dissemination and capable of transcending

both identity and culture, enabled the group to popularize its war in a manner unparalleled by any other insurgent actor, past of present".

insurgents dedicated considerable resources to develop their unique online recruitment plan. They had a strategy in place that followed a timeline for existing members and stakeholders to recruit new members and once the new members were hooked, insurgents also referred to their plan of action to predict and identify what radical actions this group was most likely to make (Berger, 2015).

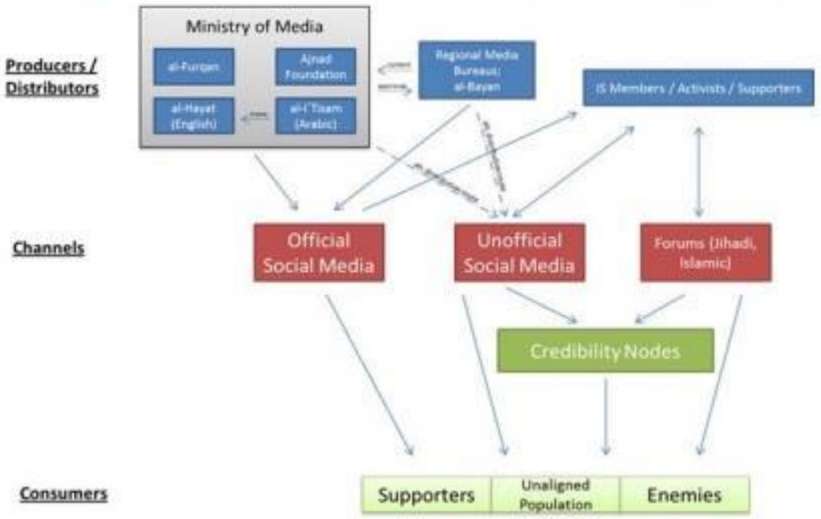
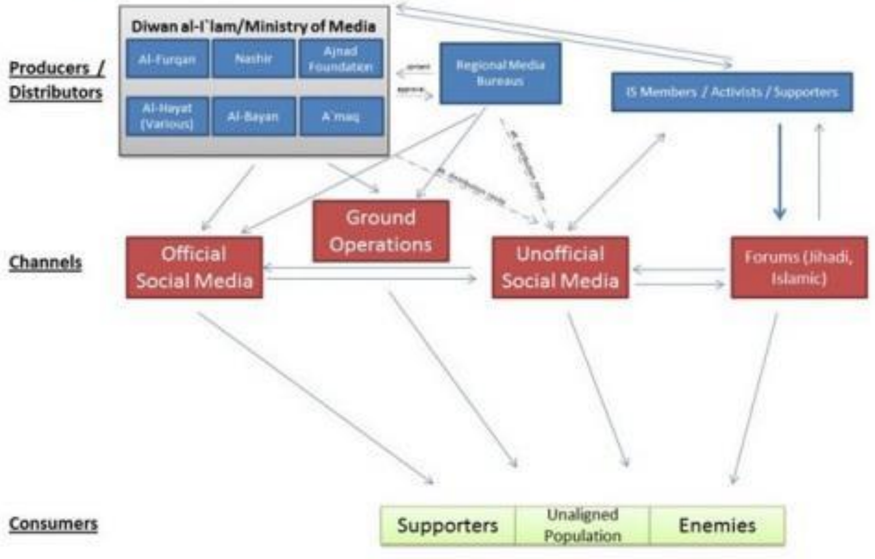


Figure 3: The Islamic State's Media Landscape (Late 2014 Representation)

Figure 4: Updated Version of Islamic State Media Landscape



Charts by Daniel Milton, 2016.

J.M. Berger (2015), who has heavily researched insurgents' online strategy has detailed step-by-step the recruitment process used by insurgents to recruit new members, in this case, Western recruits from the United States of America:

a. First contact
    i. Insurgents seeks out target
    ii. Recruiters respond to targets who seek out insurgents
b. Create micro-community
    i. Maintain constant contact
    ii. Encourage target to insulate against outside influences
c. Shift to private communications
d. Identify and encourage pro-insurgents action suitable for target
    i. Social media activism
    ii. Travel to insurgents' territories
    iii. Terrorism

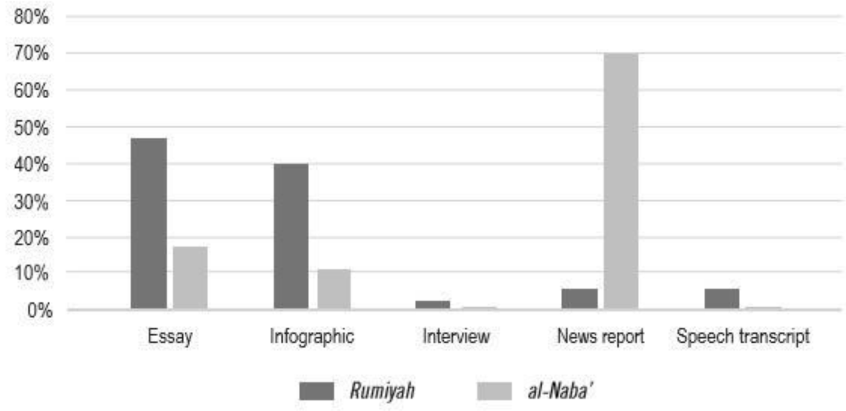
This step-by-step process describes the detailed process insurgents have developed to first brainwash vulnerable people, and subsequently recruit them. As Berger states, they make themselves ‘highly available to curiosity seekers’ which then obviously increases their success rate at recruiting new insurgent members (Berger 2015).

Simply examining this process of digitally recruiting insurgents’ members and/or sympathizers indicates how important of a role information technology plays in today’s global security crises. Previously, radical organizations would have to physically recruit members which would pose a greater security risk to them as a radical organization, and would also cost significantly more in terms of resources, logistically, time-wise, and financially. In the online world, they can hide behind the clever techniques of encryption.

3.4 The Type of Content

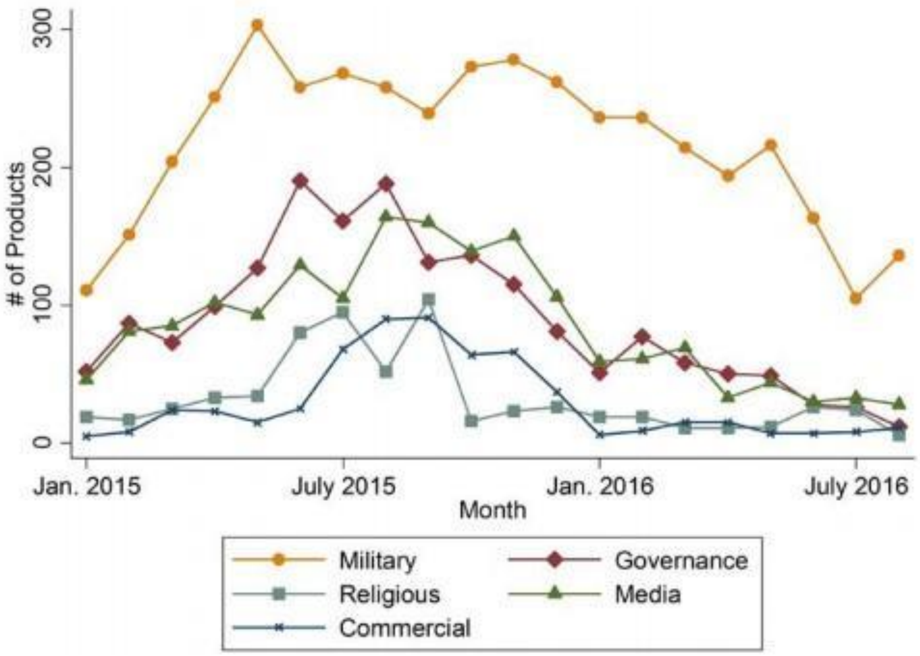
So far in this case study of insurgents we have examined insurgents’ use of information technology, we have studied how they manipulate social networks and how they recruit members. Their success in these endeavours would not have been so successful if it were not for the nature of the content they published digitally.

In this section, we will take a deep look at the type of content published by insurgents and how their information technology and media department has strategically crafted different content for different audiences.



Graph by ICSR, 2018

Figure 15: Number of Islamic State Media Products over Time, by Theme



Graph by Daniel Milton, 2016.

One of the most telling examples of the effort made by insurgents to segment their content is by simply looking at their two most prominent media publications. Insurgents have a physical newspaper which it would distribute among the towns it captured and it also had a digital magazine which it would publish online (Zelin 2015, Winter 2015; 2017). The former, the physical newspaper, would heavily focus on news items, talking about attacks conducted by insurgents. This was aimed at bolstering local supporters. However, the online magazine called *Rumiyah* was lengthier and more ideological in its content. This is because the online magazine was for *potential* members of insurgents. It was aimed at spewing propaganda that would ensnare potential members, and it was responsible for content to keep the community of insurgents' supporters worldwide still interested. The content would deal with various things such as social issues, religious issues, essays about 'Islamic' ideology. Online, insurgents' aim was to 'agitate, incite and instruct' (Winter, 2015). The aim of this magazine was to gain more supporters and as such it was impressively simultaneously published in English, French, German, Russian, Turkish, Urdu, Uyghur, Pashto, Indonesian, Kurdish and Bosnian. That is an impressive 11 languages. This indicates two things. The first, that insurgents (an originally Arabic-speaking radical organization), had a big vision of its global reach and thus empowered its members from all over the world by making them *stakeholders* in the 'vision and mission' of insurgents, so to speak. The second, is that their digital strategy was highly sophisticated and well-strategized.

The International Centre for the Study of Radicalization (ICSR) has written a detailed study of the differences in insurgents' messaging both in its physical territories and in the digital sphere. In terms of digital content, they have noted that insurgents published uniform content among its different language editions but that they also had some content that was language-specific. This indicates a high level of understanding of different cultural contexts in the members they were targeting. These strategies placed them at an advantage to counterterrorism efforts which had a lot of catching up to do to reach this level of global penetration.

The ICSR examined 13 months of issues of *Rumiyah* published by insurgents and developed a consensus on the type of content:

1. There were heavily detailed essays
2. Infographics were present

3. 47% were lengthy essays
4. 60% of the content was non-military in nature
5. The categories of this non-military content were: (largest proportion) religious advice and religious positioning, victimhood (tragedies befallen IS members/infrastructure due to the actions of 'infidels' i.e. counterterrorism efforts), history, governance, women, eulogy for martyrs, and operational advice.

We can thus see that insurgents focused heavily on a more ideological/theoretical line for their online publications as its aim was to get new members. We can also see the importance they gave to information technology's role in terrorism and counterterrorism.

3.5 Counterterrorism efforts by social networks

Previously, radical organizations would operate covertly on the online sphere, they would use password protected forums and would communicate primarily in Arabic (Winter, 2017). However, with insurgents all this changed. insurgents were the first (and will not be the last) radical group to utilize social media to its full capacity. They openly and blatantly used social networks the way they were meant to be used. They had consistent taglines and branding, they used hashtags and attempted to get them trending on Twitter and they used social media to drive more traffic to their other websites (Berger 2015).

This took the world by surprise and the social network managements themselves had a hard time not only controlling these radical propaganda efforts but also in reconciling what they were doing with their proclaimed ethos of free speech.

Twitter, for example, at first did not react to insurgents' heavy usage of its social network (Berger 2015; Winter 2015). Of all the social media networks, Twitter was the most highly used by insurgents due to the succinct nature of its platform. Twitter from its outset was committed to being a vehicle of free speech and as many of us can remember from the Arab

Spring of 2011, Twitter prided itself on being a catalyst for free speech movements. However, in this case, it was caught in a conundrum. Should it go against its ethos and start shutting down insurgents' accounts? An additional question posed by this dilemma was the reaction other regular users of Twitter would have if they saw Twitter working heavily with governments in counter-terrorism efforts. What would this mean for their privacy and the confidentiality of their data? This is a slippery slope and due to the newness and globalized nature of online social networks, it is still one that the world is unsure about.

Twitter, then faced with international government pressure and the threat of being accused of aiding and abetting radical organizations, began shutting down main insurgents' accounts. However, insurgents began consistently creating new accounts and developed a

> *"'centralized decentralization' plan, creating a number of official dissemination accounts, meaning that if one account was taken down, others will still be operational. These accounts would then tweet whenever the new account of the one taken down was back online using an alternative handle"* (Zelin 2015).

This shows insurgents' ability to consistently have an online presence and is also indicative of the nature of social networks that allow users to create and delete accounts. This strategy, in addition to clever cyber tactics of using VPNs, means that it becomes very hard for counterterrorism efforts in the field of information technology to be effective.

3.6 Cybercrime by insurgents

Compared to the significant amount of literature there is on social media usage by insurgents (Berger, 2015; Zelin, 2015; Winter, 2015; 2017), there is barely any literature on cybercrime conducted by insurgents. Admittedly, these were rarer in occurrence than insurgents' heavy use of social media, but counter-terrorism experts must spend resources to study and understand the nature of these few cyberattacks in order to be better prepared should another one strike again. In the future, not only insurgents but other radical organizations, will be depending heavily on conducting cyberattacks and in order to avoid being at a loss on how to target this issue, a solution must be found by studying past and existing examples. Cyberattacks are bound to become more popular for radicals for the very same reasons that online propaganda and recruiting was; the relative anonymity and the comparative need for less resources in order to conduct these attacks.

Through research spent reading about cyberattacks and insurgents, two conclusions can be drawn:

1. The first is that governments will take strong measures to protect themselves against portraying a weak image of their cyber defense capabilities. Anything published which indicates how their security networks were compromised will not only lead to more vulnerability for the governments themselves but will also create a chance for more attacks to take place.
2. The second is that insurgents (as with their social media tactics) like to portray a stronger image than they really are. They will edit information and publish only things that bolster themselves. Thus, they will claim many cyberattacks and it is thus a blurred line when it comes to believing whether they have *actually* conducted those attacks or if they are simply rushing to claim responsibility for attacks they weren't really involved in. This point is supported by Kyle Wilhoit, a senior security researcher, who claims that while insurgents are proficient in the use of social media, it lacks the capabilities 'to develop encryption software and malware.'

According to the online journal Strategic Culture Foundation, insurgents has claimed responsibility for several cyberattacks, some of those being:

- Jan 2015 - Twitter and Youtube account of the U.S. CentCom took over and filled with pro-insurgents' messages. The accounts were temporarily suspended for approximately 30 minutes. The United States Central Command security measures were so weak, according to insurgents, that even a two-factor authentication process was not in place (TrendMicro, 2015). According to Trend Micro, breached high-profile accounts could pass the following risks to their followers:
    - Malware infection via poisoned links
    - Spammed tweets in social feeds
    - Loss of personal information from phishing scams
    - Public shaming of specific individuals or groups
    - Dissemination of wrong, fear-mongering information to the general public
- Mar 2015 - United States Air Force's pilots list with detailed personal information posted online. In this hacking incident, photos and addresses of 70 drone pilots were released "in vindication for other insurgents' members killed in drone strikes" (AirForceTimes, 2015).
- Apr 2015 - French TV5Monde live feed and social media hacked and defaced with the message "Je Suis insurgents". This was done not only by controlling the website and social network channels of TV5Monde but also blacking out 11 of their channels (AP, 2015).
- Apr 2015 - Australian airport website defaced with insurgents' message. This seems like a strange target, however, upon further examination, experts discovered that insurgents' hacking division was arbitrarily targeting official websites that were on the

same web host, and were thus effectively targeting the web host, not the actual website (AFP, 2015).

- Aug 2015 - United States' military database hacked and data of some 1400 personnel posted online. These details included addresses, email addresses and passwords. insurgents claim they received the information from military and government databases (Safi, 2015).
- Sep 2015 - British government emails hacked. Email addresses of top cabinet ministers published.
- Apr 2016 - Successfully hacks 20 Australian business websites, redirects them to insurgents' content. This was one of the first attacks conducted by the United Cyber Caliphate (UCC) which formed in April 2016 by merging three groups, the Caliphate Cyber Army, Sons Caliphate Army and the Kalashnikov Team, which previously acted independently (Ockenden and Sveen, 2016).
- Apr 2017 - Released a kill list of 8,786 people. This list was released by the United Cyber Caliphate (UCC) and had a random amalgamation of addresses and contact numbers of mostly U.S. and U.K. individuals (Corbin, 2017).

Additionally, in December of 2017, a pro-insurgents group widely announced that they would be conducting a large-range global hack. This group, calling themselves Electronic Ghosts of the Caliphate, threatened to deface Western government websites. However, as the power and hold of insurgents had largely waned by this point, this was simply a support group of insurgents and not the main centre of insurgents' operations itself. Regardless, this goes to show that any person with radical sympathies and with coding and hacking skills can create major disruption and security breaches. The digitalization of war has made supporters and sympathizers into stakeholders with their ability to pursue the agenda of the main radical organization.

This effort at inclusion is proved by insurgents developing the UCC (United Cyber Caliphate) to act as an umbrella organization for 17 different hacker groups (Evening Standard, 2017). This has the potential to be extremely dangerous as the flow of information can spread faster between stakeholders. The Middle East Media Research Institute (MEMRI) has recently set up a Cyber and Jihad Lab project to keep track of cyberattacks conducted by radicals and on their website, they list several developments in the world of cyberterrorism, the most recent and chilling one being the following:

“An insurgents’ supporter posted a message on a pro-insurgent’ chat group recommending that lone wolf operatives use Snapchat’s Snap Map to find the most crowded places to carry out their attacks.”

This is a terrifying prospect and shows several things:

1. First, that one can simply be a supporter or sympathizer and still provide dangerous ideas.
2. Second, that social media is a breeding ground for radicals as it provides them with an arena to exchange ideas and recruit fellow members
3. Third, that the features of social media networks (in this case Snapchat’s Snap Map) can be used in a negative way to cause horrific attacks.
4. That there is no question about governments and social media networks working together to create a safer environment for its general users, as the general security of the public is now at stake due to features of these social media networks.

Chapter 4: Recommendations

There are many things that can be done to combat cyberterrorism. First and foremost, it is important for governments to recognize the extent of the security threat posed by cyberterrorism and to accordingly invest in measures to counterattack this.

As the case study in the previous section demonstrated, insurgents' success was due to their being one step ahead of the game when it came to manipulating information technology. Charlie Winter of the International Centre for the Study of Radicalisation states that the international community 'must be equally as creative and strategic-minded in its approach towards counter communications'.

In the same way that insurgents developed various content to suit their diverse audience, those in the field of counterterrorism in the digital sphere must understand that their audience is not homogenous and thus, counterterrorism efforts need to be made through a variety of mediums (Winter 2015).

A technical way in which counterterrorism experts can combat insurgents online is through 'resisting the production of nuance-less clickbait articles derived from the insurgents' propaganda' (Winter 2015). Furthermore, Alfifi and Morstatter (2018) state that using quantitative measures to analyse insurgents' recruitment and social strategies are imperative for a better understanding of how to counteract those strategies.

Governments need to realize that money has to be spent to secure themselves on the digital plane. It is no longer solely important to fortify one's defence through physical military capabilities. Larger budgets need to be allocated to combat cyberterrorism and governments must set up units for this. One such example is the UAE'S Computer Emergency Response Team (aeCERT). Part of the federal Telecommunications Regulatory Authority, the aeCERT combats all kinds of cybercrime ranging from low-level individual hacks to larger hacks that require a more concerted national effort. Having this dedicated team is essential to securing a nation.

In fighting cyberterrorism, there are two major approaches to take. The first is to combat the radicals' usage of social media to recruit members and spread propaganda. This can only be done by cooperating with the management of these social networks. However, this is a grey area as general users' security and privacy will be compromised in an effort to narrow down the radicals' accounts. Secondly, efforts must be made to fight the cyberterrorism hacks conducted by radicals.

The first method is a touchy subject, as these social networks were created to feed a desire for freedom of speech and privacy and the ability to spark social change. Having governments work heavily with these social networks in order to police the usage of these networks by radicals is highly controversial. However, governments must understand that this is a vital step necessary in their counterterrorism journey. The controversy is not only in breaching the privacy of the users of these social networks but also in crossing the line of government interference in a somewhat capitalistic 'private' enterprise. The world of social networks is in its infancy and teething problems are bound to happen as governments and the management of these social networks learn how to work with one another. Working together under the threat of cyberterrorism will act as a catalyst for these two parties to come up with innovative ways to work together without compromising the privacy of regular users. The dichotomy here is that the counterterrorism experts are concerned with 'open-source intelligence about insurgents', compared to the social networks whose priorities (mainly driven by financial aims) are in safeguarding the data of its users (Berger 2015).

One possible way to do this would be to strictly police the usage of VPNs and another would be to develop algorithms to identify and flag potentially threatening accounts. An algorithm of sorts could be used to notify the management of these social networks if there are repeated patterns of communications between for example, two particular users, coupled with the usage of VPNs. A prominent scholar in the field of cyberterrorism, who has been extensively cited in the previous section, notes in his report for the Brookings Institute that ‘approaches to the problems of extremist use of social media are most likely to succeed when they are mainstreamed into wider dialogues among the wide range of community, private, and public stakeholders.” (Berger 2015)

The research conducted by D. Milton (2016) further asserts this point by pointing out that ‘the need for both resources and flexibility suggests the importance of a public-private partnership in attacking the insurgents’ propaganda activities.’

There are many basic things that cybercrime fighting units can do to curb cyberterrorism. These are (Thuraisingham 2010):

4.1 Encryption

Encryption is the process of having a set of words or symbols that works like a private dictionary to a secret language that can only be read using that particular dictionary. Without acquiring the dictionary, you will not be able to decrypt the message. This method of encryption is used both by cyber radicals and counter radical experts. One-way cyber radicals might use encryption is by encrypting their own personal files. Another way is by hacking into their targets’ data and encrypting those files. Ransomware, a common form of cyberterrorism, relies solely on this method of encryption. For counterterrorism experts, encryption can be used to protect all sensitive files. However, a disadvantage or weakness of this method is that if the dictionary- or key- is fallen into wrong hands, the whole privacy is compromised. An example of encryption by counterterrorism experts is when the counterterrorism strategy is protected by encryption and only shared amongst stakeholders.

4.2 Network and system security

Making sure that the network and home infrastructure that you heavily rely on is protected is another significant way governments can counteract cyberterrorism. Using reputable firewalls and having them properly set up to fully utilize the advantages of having those firewalls. Having Intrusion detection systems (IDS) and intrusion prevention systems (IPS) set up properly to inform and provide continuous feedback to the system administrators is another way to protect governments and other entities against possible hacking. Additionally, utilizing a SIEM (system intelligent event management) to draw out anomalies and have a dynamic view of your system hierarchy and to reverse engineer any possible attempt to hack your infrastructure and to reverse engineer intruder hacks.

4.3 Application security

Application security is a continuous process of refinement where applications are constantly monitored by administrators for weaknesses and vulnerabilities. Through a constant process of revision, many common flaws can be detected or rediscovered after initial checks. This continuous process helps fortify government systems against problems faced by weaknesses in the system. According to Improving Web Application Security book, some of these common flaws are:

Category	Threats / Attacks
Input Validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Software Tampering	Attacker modifies an existing application's runtime behavior to perform unauthorized actions; exploited via binary patching, code substitution, or code extension

Authentication	Network eavesdropping; Brute force attack; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive information	Access sensitive code or data in storage; network eavesdropping; code/data tampering
Session management	Session hijacking; session replay; man in the middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

4.4 **Datamining** (both traditional and real-time data mining).

Datamining is an essential process of general cybersecurity housekeeping and upkeep. The premise of data mining is to have a continuous feedback on the security situation of a particular software or system. Data Mining mines and sifts through millions of bytes of raw data on a daily basis and uses algorithms to detect anomalies. Security intelligence event management (SIEM) systems such as LogRhythm are types of data mining software used by cybersecurity teams in their protection efforts. The bytes of data analysed by these SIEM systems are called critical security logs. These are subsequently analysed by classification and graph mining to detect abnormalities. The critical security logs are searched in different classifications, some of them being: URL logs, duration logs, classification logs, direction logs, and port logs.

Lesser-developed countries also have to catch up by first investing in standardization and access, and primarily better bandwidth to target these efforts.

However, with the nature of the internet, “using repressive measures such as criminalization of online activities is not necessarily the most suitable solution…as it is not effective, since other methods will quickly replace [the] blocked options (van Ginkel).
(Provide example of Bangladesh hack).

“Cyberterrorism is a more realistic option than it was ten years ago, and it is about time to establish more sophisticated and flexible cybersecurity measures to ensure…security.” (Mediterraneanaffairs.com). The United Kingdom is one nation who is heavily relying on conducting cyberattacks themselves to limit the online capabilities of radicals. The Government Communications Headquarters (GCHQ) has engaged in several high-profile attempts to curtail the online abilities of insurgents, according to its current head, Jeremy Fleming. David Bond of the Financial Times has written about Mr. Fleming’s comments at a CyberUK conference in 2018. Mr. Fleming listed the primary activities that the government would do to combat cyberterrorism and these are:

1. Denying service
2. Disrupting specific online activities
3. Deterring an individual or group

4. Destroying equipment or networks

As can be seen, there are several important measures which can be adopted by counterterrorism experts to not only defend itself against cyber radicals but also to conduct attacks of their own and limit the capabilities of these cyber radicals. It would require governments not only joining hands with social media networks but also it would require the development of sophisticated digital strategies to thwart and attack cyber radicals.

Chapter 5: Conclusion

To conclude, it is clear to see that the information technology revolution has caused the political world order to change. IT has given access to individuals to spark their own social and political change and as we have seen with the case of insurgents, this access can often be abused. Warfare in the 21st century has fundamentally changed due to the emergence of many groups of violent non-state actors, but also due to their appropriation of technology as a both a means to an end and as an end in itself.

It is imperative for governments the world over to readdress how they perceive their security and they must place a premium on the importance of cybersecurity. Governments and other important entities need to extensively develop their cybersecurity capabilities by investing in digital counterterrorism units in order to thwart cyberattacks that can undermine their overall security.

Social media networks have indirectly disrupted counterterrorism efforts as radical groups such as insurgents have used these very networks to further their reach. It is a grey and controversial zone but governments need to work together with the management of social media networks in order to prevent and limit the ability of radicals to use these channels for propaganda and recruitment.

A globally concerted effort is required to counteract cyberterrorism in order to prevent the example of insurgents' usage of IT to become the norm. There is much scope for future study and the success of this is ultimately dependent on global governments' willingness to cooperate.

References

1. Alfifi, Morstatter, et al. (2018). Measuring the Impact of insurgents Social Media Strategy. Stanford: CA: Stanford Network Analysis Project. Available from: http://snap.stanford.edu/mis2/files/MIS2_paper_23.pdf
2. Alfifi, M. and Caverlee, J. (2017). Badly Evolved? Exploring Long-Surviving Suspicious Users on Twitter. In International Conference on Social Informatics. Springer, 218–233
3. Awan, I. (2017). "Cyber-Extremism: insurgents and the Power of Social Media", Social Science and Public Policy, Vol. 54, pp. 138-149.
4. Badawy, A. and Emilio Ferrara. (2017). The Rise of Jihadist Propaganda on Social Networks. (2017).
5. Benigni, M. and Carley, K. M. (2016). From Tweets to Intelligence: Understanding the Islamic Jihad Supporting Community on Twitter. In Social, Cultural, and Behavioural Modelling: 9th International Conference, SBP-BRiMS 2016, Washington, DC, USA, June 28-July 1, 2016, Proceedings 9. Springer, 346–355
6. Berger, J.M. and Morgan, J., (2015). 'The insurgents Twitter Census: Defining and describing the population of insurgents supporters on Twitter'. Washington, DC: Brookings Institution. Available from: www.brookings.edu/wp-content/uploads/2016/06/insurgents_twitter_census_berger_morgan.pdf
7. Berger, J.M., (2015). "Tailored Online Interventions: The Islamic State's Recruitment Strategy," CTC Sentinel, Vol. 8, Issue 10, October 2015, p. 19-23, available at: https://www.ctc.usma.edu/posts/tailored-onlineinterventions-the-islamic-states-recruitment-strategy.
8. Berger, J.M. and Morgan, J. (2015). "The insurgents Twitter Census," Centre for Middle East Policy at Brookings, No. 20, March 2015, available at:

https://www.brookings.edu/wp-content/uploads/2016/06/insurgents_twitter_census_berger_morgan.pdf.

9. Brunst, P. W. (2010). Terrorism and the internet: New threats posed by cyberterrorism and radical use of the internet. In A War on Terror? (pp. 51-78). Springer New York.
10. Burke, J. (2016).“The Age of Selfie Jihad: How Evolving Media Technology Is Changing Terrorism,” CTC Sentinel, Vol. 9, Issue 11, November/December 2016, p. 16-23, available at: https://www.ctc.usma.edu/v2/wp-content/uploads/2016/11/ CTC-Sentinel_Vol9Iss1113.pdf.
11. Carter, J., Maher, S. and Neumann, P., (2014). #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks. London: International Centre for the Study of Radicalisation and Political Violence, King’s College. Available from: icsr.info/wp-content/uploads/2014/04/ICSR-Report-GreenbirdsMeasuring-Importance-and-Infleunce-in-Syrian-ForeignFighter-Networks.pdf
12. Conway, M., Khawaja, M., Lakhani, S., Redfin, J., Robertson, A. and Weir, D., (2017). Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts. VOX-Pol. Available from: www.voxpol.eu/download/vox-pol_publication/DCUJ5528- Disrupting-DAESH-1706-WEB-v2.pdf
13. Conway, M. (2002). Reality bytes: Cyberterrorism and radical ‘use’ of the Internet. First Monday 7(11) Retrieved 15. 05. 2015 from http://firstmonday.org/ojs/index.php/fm/article/view/1001/922
14. Corbin, C. (2017). Pro-insurgents hackers release kill list with 8,786 targets in US, UK.
15. Diresta, R. (2018). The Information War is On. Are we Ready for it? Wired.com

16. Ferrara, E. Wen-Qiang Wang, Onur Varol, Alessandro Flammini, and Aram Galstyan. (2016). Predicting online extremism, content adopters, and interaction reciprocity. In International Conference on Social Informatics. Springer, 22–39.

17. Ferrara, E. Wen-Qiang Wang, Onur Varol, Alessandro Flammini, and Aram Galstyan. 2016. Predicting online extremism, content adopters, and interaction reciprocity. In International Conference on Social Informatics. Springer, 22–39.

18. Goldstein, J. S., Pevehouse, J. C. W. (2012). International Relations. London, UK: Pearson.

19. ICSR. (2018). A Tale of Two Caliphates: Comparing the Islamic State's Internal and External Messaging Priorities. London: International Centre for the Study of Radicalisation, King's College. Available from: https://icsr.info/2018/07/23/a-tale-of-two-caliphates-comparing-the-islamic-states-internal-and-external-messaging-priorities/

20. Klausen, J., (2015). 'Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq'. Studies in Conflict & Terrorism, 38 (1), pp. 1–22.

21. Magdy, W., Darwish, K., and Weber, I. (2015). # FailedRevolutions: Using Twitter to study the antecedents of insurgents' support. (2015).

22. Meier, (2003). Improving Web Application Security: Threats and Countermeasures. London, UK: Microsoft Press.

23. Milton, D., (2016). Communication Breakdown: Unravelling the Islamic State's Media Efforts. West Point, NY: Combating Terrorism Center, United States Military Academy. Available from: ctc.usma.edu/

24. Nye, J. S. (2010). Understanding International Conflicts. London, UK: Longman.

25. Ogun, M. N. (2012) Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, Journal of Applied Security Research, 7(2). 203- 217, DOI:10.1080/19361610.2012.656252
26. Pavey, H. (2017). insurgents being hindered by 'really, really bad' coding skills. Eveningstandard.com
27. Rayamajhi, S. (-). A Synopsis of Cyber Warfare and Terrorism. Diplomacy Foundation.
28. Rothenberger, L. (2012). Terrorist Groups: Using Internet and Social Media for Disseminating Ideas. New Tools for Promoting Political Change. Romanian Journal of Communication and Public Relations. 14(3).
29. Safi, M. (2015). insurgents 'Hacking Division' releases details of 1,400 Americans and Urges Attacks. Theguardian.com
30. Thuraisingham, B. (2010). Selected Topics in International Terrorism and the Application of Information Technology: Volume 1: Terrorism Tactics, Trends, and Technologies.
31. Tumbul and Akdogan, (2016). "How do radical organizations use Information Technologies?", Middle East Review of Public Administration, Vol 1, Issue 1, 2016, pp. 2-16.
32. University of Oslo, Jihadi Document Repository, available at: http://www.hf.uio.no/ikos/english/research/jihadi-document-repository/ index.html.
33. Veerasamy, N., Grobler, M. (2011). Terrorist Use of the Internet: exploitation and support through ICT infrastructure. Available from researchspace.csir.co.za
34. Von Clausewitz, C. (1832). On War. London, UK: Penguin Random House.
35. Weimann, G. (2009). Terror on facebook, twitter, and youtube. Spring 16(2), 45-54

36. Winter, C. 2015. Documenting the Virtual ‘Caliphate.’ London: The Quilliam Foundation. Available from: www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documentingthe-virtual-caliphate.pdf

37. Winter, C. (2015). “The Virtual Caliphate: Understanding Islamic State’s Propaganda Strategy,” The Quilliam Foundation, July 2015

38. Winter, C. (2017). Media Jihad: The Islamic State’s Doctrine for Information Warfare. London: International Centre for the Study of Radicalisation, King's College. Available from: icsr.info/wp-content/uploads/2017/02/Media-jihad_web.pdf

39. Zelin, A., (2015). ‘Picture or it didn’t happen: A snapshot of the Islamic State’s official media output’. Perspectives on Terrorism, 9 (4). Published online. Available from: www.terrorismanalysts.com/pt/ index.php/pot/article/view/445/html

40. Zhao, V. H., Lin, W. S., & Liu, K. J. R. (2011). Behavior Dynamics in Media-Sharing Social Networks. Cambridge: Cambridge University Press.

41. -, (2017). insurgents Warns of Imminent Cyber Attacks on the U.S. Cybersecurityintelligence.com

42. -, (2015). US Central Command Hack: A Warning for High Profile Accounts. Trendmicro.com

43. – (2015). Australian Airport website hacked by Islamic State. Telegraph.co.uk

44. – (2015). insurgents-allied Hackers claim worrying new attack. CBS.com

45. – (2018). insurgents again claim cyber attacks which were falsely blamed on Russia. Strategic Culture Foundation.