The Cyber Phenomenon of the Islamic State – What the West Must Understand

Daniel Bren and Yossi Levy¹

“The Islamic State is expert in communications and instilling fear. There is no real reason to be afraid of them.”

Major-General (res.) Amos Yadlin, former chief of the IDF’s Military Intelligence Directorate and Executive Director of Israel’s Institute for National Security Studies (INSS), in 2014.²

“The terror group known as ISIL must be degraded, and ultimately destroyed.”

President Barack Obama addressing the UN General Assembly, 2014.³

In 2014, Western and Arab nations led by the United States and the United Kingdom committed to combat and defeat the terror group the Islamic State or ISIL (the Islamic State in Iraq and the Levant). These allies even sought out a new partnership with Iran, an arch-rival, to defeat their common enemy. On the sidelines of the 2014 UN General Assembly, the British prime minister and the president of Iran met for the first time in the thirty five years since the Islamic Revolution to discuss strengthening common ties against IS.⁴ The New York Times reported that American forces attacked the Islamic

¹ Brigadier General Daniel Bren is currently head of “Lotem,” Unit for Telecommunications and Information Technology at the J6/C4i. Mr. Yossi Levi a cinema director, scriptwriter and editor, specializing in the Mass Media.
² Major-General (res.) Amos Yadlin at a conference on ISL, January 5, 2014.
⁴ “An hour of practical dialogue,” tweeted Rouhani. “A small piece of history has been made,” said Cameron.
State from the air while Iranian forces maneuvered against the group from the ground.

Only four years earlier, US President Barack Obama fulfilled his campaign promise to remove American forces from Iraq and pledged to avoid future military entanglements in the Middle East. While the Syrian civil war claimed hundreds of thousands of lives and displaced millions, the United States and other Western nations essentially stood by and did nothing. But now, the United States was leading a new coalition of Western nations and Arab allies to combat a terror organization from those very same lands from which the Americans only recently withdrew.

What brought Western nations to engage in a new Middle Eastern fight that could take, according to both the British PM and the US Chairman of the Joint Chiefs of Staff, many years and the presence of tens of thousands of ground troops? How is it that in such a short time a terror organization, whose existence was only recently discovered, whose members number less than 40,000, which employs elementary weapons and pickup trucks, came to be considered a threat to the United States and other Western nations? What brought these states to ally with and even strengthen those very countries deemed, only a decade earlier, the ‘Axis of Evil,’ principal among them Iran?

The answer lies in the Islamic State’s sophisticated, innovative and coordinated use of modern channels of communication in cyberspace. The Islamic State succeeds in frightening the West as no other terror organization has before because it is the first to successfully take advantage of modern platforms while demonstrating the patience and stamina to achieve its revolutionary goals of restoring the Muslim Caliphate. The West not only struggles to understand the basic ideological foundations of the Islamic State, it fails to understand how the organization takes advantage of 21st-century technologies. The West’s unfamiliarity with the Islamic State’s aims and means not only leads to unnecessary fear, it hampers efforts to counter the Islamic State and perhaps, paradoxically, even strengthens the terror organization.

This paper reviews the ideological and theological foundations of the Islamic State and examines how the Islamic State deftly utilizes modern cyberspace to further its global ambitions. By understanding
the sources of the Islamic State’s strength, principally in the cyber realm, Western states can be better equipped to more accurately comprehend the scope of threat posed by the Islamic State threat and better prepare themselves to counter the terror group’s activities.

The Islamic State Phenomenon
The Islamic State is an extremist Sunni terror organization founded on a defined and ordered theology. Contrary to popular belief, this organization did not emerge recently or from nowhere. It holds deep roots in extremist Sunni thought and terror groups. Islamic State leadership worked for years to hone its strategy and tactics before it formally declared the establishment of a new Caliphate in June 2014. Today, the Islamic State fights for a global Muslim revolution, what it calls the ‘Rise of the Ummah (the community of Muslims)’ to re-establish the Islamic sovereignty and build a model fundamentalist Islamic society. The Islamic State inspires Muslims around the world who feel persecuted and suppressed to join its holy cause of world domination under the flag of Islam.

Abu Musab al-Zarqawi founded the organization Jama’at al-Tawhid wal-Jihad (the Organization of Monotheism and Jihad) in 1999 in Jordan with the initial goal of overturning the Hashemite Kingdom. Following the American-led campaign in Afghanistan and the beginning of the Global War on Terror, Zarqawi moved his operations to Iraq. During the 2003 American-led invasion of Iraq, Zarqawi committed his loosely networked organization to fighting the coalition forces who invaded to overthrow Saddam Hussein’s regime. In 2004, the organization swore allegiance to the Al Qaeda group and became known as Al Qaeda in Iraq. Al-Zarqawi was killed in a US air strike on June 8, 2008 and was replaced by Abu Ayoub al-Misri, who also killed in a joint American-Iraqi action in April 2010. Abu Bakr al-Baghdadi took over from al-Misri in 2010.

Abu Bakr al-Baghdadi shifted the organization’s strategy and operating principles. Moving away from traditional guerilla-type terror activities, al-Baghdadi sought to seize and control land in Iraq and build the foundations of a fundamentalist Islamic society, a restored Islamic Caliphate. He committed to governing these areas
under strict Islamic rule while fighting to expand his territorial reach. In light of this new focus, the organization changed its name to the Islamic State of Iraq and later the Islamic State of Iraq and the Levant (ISIL) to reflect its new strategic aims. ISIL split from Al Qaeda in 2014 following disagreements between central Al Qaeda leaders and field commanders. In June 2014, ISIL simplified its name to the Islamic State, demonstrating its growing ambitions to establish an independent Islamic Caliphate and to inspire worldwide Muslims to join its cause.

The Islamic State views its operations in three geographical spheres of influence. Within the first sphere, the nucleus of the organization in Iraq, Syria, and Afghanistan, the Islamic State consolidates its control and develops the political and social model that inspires future expansion. The Islamic State primarily focuses its expansion into the second circle, the Muslim states perceived to have gone astray from the true ways of Islam. The third circle is the non-Muslim world, particularly the West. Although the West is not the priority target for expansion, as shown later in the article, one should make no mistake that the Islamic State is waiting to exert its influence in Western countries.

While this ideology of spheres of influence is found at the heart of many different Islamic terror groups from Al Qaeda to Hezbollah, the Islamic State has proven the most successful to deploy cutting-edge twenty-first century technologies to penetrate and make waves in all of three of those spheres simultaneously.

**The Cyber Dimension**

For centuries, chants and the beat of war drums over battlefields accompanied the advance of conquering armies. Today, technology and the evolution of the internet herald a new era of warfare in which the personal computer, the mobile cellular device and social networks play central and critical roles in the implementation and realization of military strategy.

At the beginning of the twenty-first century, researchers identified that terror organizations used the internet for five principal purposes: propaganda and psychological warfare, recruiting members, raising funds, information gathering, and executing operations. In the early 2000s, terror groups operated
quietly and used traditional technologies such as e-mail, web sites and online forums.\textsuperscript{5}

When the Web 2.0 revolution\textsuperscript{6} arrived, the traditional rules for online terror changed dramatically. The Islamic State fully grasped the enormous potential presented by the rise of social networks, high-speed internet, mobile devices, and the globalization of the web. Al Qaeda was among the first terror organizations to successfully employ internet technologies, particularly as a means of communication, command, control, and instruction. The Islamic State surpassed Al Qaeda both in scope and sophistication in its utilization of cutting-edge technologies for both outreach and military operations.

**Propaganda 2.0**

Propaganda, the use of mass communications tools to influence public behavior, has existed for thousands of years. Successful propaganda repeatedly transmits a single message across many distribution channels over an extended period of time to amplify the message’s exposure. Eventually, the message enters the subconscious. The centrality of propaganda to the rise of the two major totalitarian regimes of the twentieth century, Nazi Germany and the Soviet Union, is well known. The ideological foundations of these regimes demanded the creation of a sense of a collective, unifying and all-encompassing national narrative and creed. The success of these regimes in their rise to power was largely due to the successful employment of the modern technology of the time: cinema and radio. Complemented by mass rallies and symbols that created a visual and ideologically idiosyncratic language, the regime’s ideology spread through all aspects of life.

Like the totalitarian regimes of the twentieth century, the Islamic State thoroughly understands the significance of modern communications tools and their potential to influence human activity. The Islamic State created a modern, sophisticated and well-coordinated online propaganda campaign that embraces all modern


\textsuperscript{6} Web 2.0 refers to websites that promote user-generated content, social networks, usability, and interoperability on across multiple platforms and devices.
internet channels and social networks (such as WhatsApp, Facebook, Twitter, and YouTube), for the distribution and promotion of its Jihad brand all over the world.

One needs to look no further than the evolution from al-Zarqawi’s Al Qaeda in Iraq to al-Baghdadi’s Islamic State to understand how the Islamic State surpassed other groups in its use of technology for propaganda.

In September 2004, al-Zarqawi kidnapped and beheaded two Americans and one Briton. The videos of the execution were posted to internet sites and quickly discovered by global television networks, who broadcast the story and the gruesome videos widely. The story garnered attention for about a week, but was quickly eclipsed by other news and atrocities.

A decade later in 2014, al-Baghdadi’s Islamic State re-enacted similar scenes. One after another, the Islamic State filmed the executions of American photographer James Foley, American journalist Steven Sotloff, British aid worker David Haines, and uses British journalist John Cantlie for propaganda videos. Each execution video features repeated and striking motifs—the victims wore orange jumpsuits (reminiscent of the prisoners held by American forces at Guantanamo Bay) and stood before a black flag with the Islamic State logo. The gruesome videos led Western leaders to call for decisive action against the Islamic State. So, one must ask the question, why would similar tactics used in 2004 and in 2014 be treated differently by the West?

The power of social networks and their centrality in our daily lives, alongside video-sharing web sites, and the birth of the “blogosphere,” freed the Islamic States from its previous dependence on mainstream news outlets and allowed these videos to spread rapidly and virally. Today, the Islamic State operates independently in all forms of the media (written, audio and video) through the internet. The Islamic State employs experts skilled in the latest production, editing, and marketing techniques. The organization stays at the cutting edge of technologies to exploit latest trends such as #hashtaghijacking,7 hacking personal mobile

---

7 The hashtag is a content label from social networks that helps those interested in a particular topic to find content on that topic “Hashtaghijacking” is the use of a
accounts, deploying BOT networks,\textsuperscript{8} and gamification.\textsuperscript{9} The Islamic employs all of these means to build its legitimacy, recruit new members, raise money, and instill fear among its enemies.

**Jihad: The Video Game**

The Islamic State encourages new members to join its march toward the traditional Sunni apocalypse through high quality films and video games. While remaining true to its core theology, the Islamic State creates the impression that joining the fight in Syria or acting at home is as easy and fun as taking a vacation to Disneyland.

Nowhere is this theme more evident than in the series of films produced by the Islamic State. Most prominent of these films was the “Clanging of the Swords,” a series of four hour-long films. The first three films contain apocalyptic motifs and symbols taken from the Hadith, the sacred Sunni collection of religious laws and stories about the Prophet Mohammed, that herald the coming of the Mahdi, the Muslim Messiah.\textsuperscript{10} The films feature the black flag of the Islamic State, the organization’s online magazine Dabiq, the use of the term *Ummah*, and a red flag that represents the Mahdi, whose coming signals the end of the world. The clips are enriched by scenes of violence inspired by the popular video game series *Grand Theft Auto (GTA)* and *Call of Duty*.\textsuperscript{11}

\footnotesize{\textsuperscript{8} BOT networks, also called botnet or bot net, are a network of computers compromised by malicious code that work together to collectively perform task assign by the network’s controller.  
\textsuperscript{9} Gamification is the application of game-design elements and game principles in non-game contexts. Gamification commonly employs game design elements to improve user engagement, organizational productivity, flow, learning, employee recruitment and evaluation, ease of use and usefulness of systems, physical exercise, traffic violations, and even voter apathy, among others.  
\textsuperscript{10} As a law codex, the hadith is second only to the Koran in religious importance.  
\textsuperscript{11} GTA (Grand Theft Auto) is a billion-dollar action-adventure video game franchise, in which players navigate fictional cities to rise through the criminal underworld via crime and violence. Call of Duty is also a billion-dollar first-person shooter video game franchise that simulates modern warfare. Both games have online, networked elements in which players may cooperate or compete with other players.}
The fourth film in the “Clanging of the Swords” series takes a quantum leap from its precursors. The film presents the apocalyptic vision of the Ummah along with its achievements during the holy war toward victory. The film integrates elements inspired by the popular video game GTA IV. One scene that depicts a drive-by shooting inspired by GTA went viral on the internet in a matter of weeks. Millions all over the world viewed and shared the clip on Facebook, Twitter, Youtube, WhatsApp, e-mail, underground sites and gamers’ forums.

In the beginning of July 2014, the Islamic State released a new film called Flames of War. Unlike its predecessors, the film targets non-Muslim Western audiences. Translated entirely into English, the film features an English-speaking protagonist and is more restrained in its depiction of violence and mayhem. The combat scenes appear polished and quite similar to the Call of Duty first-person shooter video game.

via the internet. Both games are available on a wide range of platforms including PC, Xbox and PlayStation.
In mid-September 2014, the Islamic State released a video trailer for a game called Grand Theft Auto: Salil al-Sawarem [Sound of Swords]. Scenes in the promotional video clip are taken directly from the original GTA game but feature acts of jihad including an Islamic fighter shooting police officers and blowing up convoys. Jihadist fighters even shout “Allahu Akbar” while attacking a city in the United States. When describing the clip, the Islamic State said that its combatants act on the battlefield just as young gamers do while playing at home. The Egyptian media reported that the game and the video clip was meant to “raise the morale of the Mujahedeen, to train children and young people to fight the West, and to strike terror in the hearts of the enemies of the [Islamic] State.”

The Islamic State also aims to build legitimacy among skeptical Muslim populations. One of the more interesting internet campaigns of 2014 featured “the first Jihad Hipster.” A young Egyptian Islamic State recruit named Islam Yaken was filmed boasting about a beheading he had recently committed while sporting an Afro-style haircut, thick black glasses and a “hipster” look that would have made him seem cool to any Western audience. Soon pictures of the jihadi hipster sprouted all over the internet turning him into a cultural hero, with whom Western youngsters could easily identify.
In the last two years, Sunni Muslim organizations in England held “Evenings of Repentance” for young people, called “Call of Duty: Rise of the Ummah.” These evenings were promoted by video clips and posters based on graphics taken directly from the successful video game series. Currently, some of these organizations serve as the foremost representatives of the organization in its struggle for legitimacy in the British media.

The Islamic State has also used internet-based games, especially the online versions of Call of Duty and GTA, to establish contact with potential recruits and sympathizers around the world. In England in June 2014, a father claimed that his two teenage sons were tempted by the Islamic State after receiving copies of the popular video game Call of Duty: Ghosts as a present. In October 2013, a young Scot reported to police that he was asked to contribute money or join the Islamic State by an anonymous online party while playing the online version of Call of Duty: Ghosts on his Xbox console. In Australia,
federal police arrested two suspected Al Qaeda members and confiscated PlayStation 3 consoles.

Illustration 4: A Poster for Cyber Jihad based on the game Call of Duty: Black Ops

Western intelligence and diplomatic agencies are also striking back on these platforms. Following the Edward Snowden revelations, the West’s top intelligence agencies, including the NSA and the British GHCQ, admitted that they had penetrated game servers and online gaming communities in order to monitor potential terrorist activity. In addition, Snowden revealed that intelligence organizations, led by the CIA, cooperated daily with internet companies such as Twitter to close accounts associated with Islamic State and spread counter-information against the Islamic State. DARPA, the Pentagon’s research and development agency,
financed a series of projects to better understand and influence social networks.

Illustration 5: Invitation to an Evening of Repentance, in the style of Call of Duty

Recently, the US State Department distributed a video clip similar to the Islamic State’s Flames of War that exposed the atrocities being committee by the Islamic State. While the US Department of Homeland Security issued a white paper about the dangers of internet-based games as a recruitment platform as early as 2009, this was not taken seriously by intelligence and security agencies until recently.

In addition to the internet and computer games, the Islamic State also distributes mobile applications via Google Play, the online store for the Android mobile platform. One of these mobile applications, the Dawn of Glad Tidings, magnifies the organization’s profile
through social networks. The application allows the Islamic State to access the mobile user’s device data and spread information through the mobile user’s device. By utilizing such mobile applications, the Islamic State multiplies its tweets to reach hundreds of thousands around the world, making the content incredibly popular.

Jihad Tourism
The Islamic State’s propaganda and recruiting activities gave birth to a new phenomenon of Jihad tourism, or, as they call it in England, “Five-Star Jihad.” The Islamic State welcomes young potential jihadis, usually men, to visit the war-torn areas to take part in a combat adventure alongside the terror organizations. The CIA claims that over fifteen thousand foreign terrorists, from over eighty countries, are fighting in Iraq and Syria. In addition to Jihadi John from the United Kingdom, there are further examples, such as Kiwi Jihadi from New Zealand, and youngsters from Australia. Many of these young ‘tourists,’ usually educated and socially normal, return home from Syria, Afghanistan, and Iraq and enjoy immunity for any crimes committed because their home states hold no extradition agreements with war-torn countries. A prime example of this phenomenon is a seventeen-year-old Australian who went to fight in Syria after viewing one of the Islamic State’s online videos in June 2013, and pledged to fly the ISIS flag over Buckingham Palace.

Exporting Jihad
The Islamic State actively recruit jihadis to operate in the second and third spheres of influence via innovative technological means. The CIA claims that online recruitment may have a viral effect on those interested in jihad. There is ample evidence of this phenomenon in the West. In the United States, two American citizens in Boston inspired by the Islamic State online murdered four people at the Boston Marathon. Following his arrest, the surviving terrorist confessed to acting in response to events in the Middle East and that his actions were only a small part in the Jihadi effort. The brothers who attacked the Boston Marathon were later linked to an Islamic State cell. A worker in Oklahoma, fired from his job at a food processing plant in Oklahoma, beheaded his former colleague after seeing an Islamic State video clip. A young man attacked police in New York City with an axe. A series of murders in Canada and a
shooting attack on the Canadian Parliament were also traced to the Islamic State. Whether inspired directly by Islamic State propaganda or not, the Islamic State brand appears to be infectious.

Among those joining the organization in the West are many young people who were born in the West to Muslim families. However, alongside them there is a swelling tide of Christian and Jewish converts to Islam who publish their conversion online through Islamic State propaganda. Some of them join the fighters in Iraq and Syria, while others are active in their home countries. The head of the FBI said that the American authorities know of at least twelve Americans fighting alongside the extremists in Syria and more than one hundred Americans who were arrested attempting to enter Syria. He added that all Americans who had returned from Syria after fighting alongside the extremists, are under surveillance, being investigated or under arrest. Similar concerns are reported in Britain, New Zealand, Australia and other Western countries.

Cyberspace is a dimension invented by humans based on computers (hardware and software) and communications. Independent of geographic boundaries and modern conventions of governability, cyberspace hosts a wealth of information and human activity. Cyberspace enables users to create and administer communities, exchange ideas, share information, provide social support, conduct business, create art, play games, and engage in political debate.

In recent years, cyberspace has also become a war fighting domain. Cyber war may take place solely within or be deployed in support of traditional warfare on land, air, and sea. Cyber technologies may be used at the outbreak of hostilities or as a dimension in an inter-war campaign. Both states and non-state actors may employ cyber means. Cyberspace warfare is growing and dramatically changing the nature of warfare and its challenges.

“In my opinion, cyber will, in a short while, be discovered to be a greater revolution than even gunpowder, whose influence will be more significant than that which led to the attempt to use the aerial dimension in warfare at the beginning of the twentieth century.”
Traditionally, cyber warfare referred to three types of operations: Computer Network Exploitation (CNE) – intelligence-gathering operations; Cyber Network Aggression (CNA) – cyber attack; and Cyber Network Defense (CND) – defense in cyberspace. In recent years, another important type of operation has emerged: Computer Network Influence (CNI).

Many countries, Israel included, have invested significant efforts to prepare themselves for the cyber age. In the IDF, responsibility for the various layers is divided between the Intelligence and the Computer Service directorates. It is important to point out that in addition to the IDF, there are other entities in Israel that deal with cyber defense, including the General Security Service, the Ministry of Defense, the Ministry of Justice and the Israel Police. Since its establishment in 2011, the National Cyber Bureau leads cyber activity in Israel. Recognizing the need to upgrade the national preparedness in the cyber domain, Prime Minister Benjamin Netanyahu, announced the establishment of the National Cyber Authority in 2012. Despite the great interest in developing cyber warfare capabilities, most government efforts focus on the first three types of cyber warfare activity (CNE, CAN and CND) and have only recently begun to realize the potential potency of CNI activities.

The Islamic State developed a weapon that is a thousand times more significant and more dangerous than the number of small arms or trucks at its disposal - its ability to employ the latest development in cyber warfare: computer network influence (CNI). By exploiting global communications systems using both newer methods based on games and Web 2.0 technologies and other more conventional means based on social networks, the Islamic State deployed a coordinated, diverse and massive propaganda and outreach campaign. The Islamic State’s technologically driven online propaganda campaign is likely to be one of the most formative events of the coming years.

12 Major-General Aviv Kochavi, former chief of intelligence branch of the IDF, in a speech to the INSS conference, January 2014.
Western security services that identified the Islamic State’s growing online presence phenomenon did not believe in the organization’s intentions nor in its ability to create such significant waves globally. And today, the coalition against the Islamic State, led by Western and Arab leaders, launched an extreme military action at a very high cost to the taxpayers, at least ten million dollars a day. But perhaps the West is missing the core of the Islamic State’s power: its activity in cyberspace. The West has made these mistakes before.

The impact of the social networks in the age of Web 2.0 has not yet been investigated by Western agencies in depth. There is no doubt, for example, that the social networks played a historic role in the Egyptian revolution. A protest that started on Facebook and Twitter brought the end of the Mubarak regime. This was not the first time that social networks served as an instrument for virtual and popular campaigns, but it was the first time that the voice of the masses turned into joint action. Hundreds of thousands of activists were recruited and unified through the Facebook page “We are all Khaled Said.” On January 25, 2011, the masses crossed the boundaries of cyberspace and began to gather in Tahrir Square, which eventually brought the end of the Mubarak regime.

Appearing before the intelligence sub-committee of the Israeli Parliament’s Foreign Affairs and Defense Committee, the then-incoming Head of Military Intelligence, Major General Aviv Kochavi, argued that “there is no danger to the stability of the regime in Egypt,” adding, “we do not see the Muslim Brotherhood as a force sufficiently organized or unified to seize power; although, if there were elections, it would receive 40% of the vote.” The dramatic events in Egypt demonstrate that we find it difficult to grasp the power of social and virtual organizations, and even more difficult to imagine the revolutions which they can bring about.

Leaders of the West struggle to believe that beheadings and axe attacks are part of a rational decision to kill enemies in the name of

---

13 A young man murdered by police officers in Alexandria about a year and a half prior to the revolution.
http://www.nrg.co.il/online/1/ART2/206/466.html
Islam. It is much easier to sleep at night if one believes that mentally disturbed lone wolves are responsible for these attacks. It is much harder to grasp that an organized religious, nationalist movement with thousands of adherents is prepared to kill and die at the command of its charismatic leader, especially when those instructions are transmitted to them on Twitter.

Western policy toward the Islamic State and Iraq took a dramatic turn in 2014 because Western leaders began to appreciate the true depth and power of the global, networked and sophisticated Islamic State. The US president chose to return American forces to Iraq because he saw understood that the Islamic State is not a passing fad. He saw that the terror group is an advanced, well-managed organization that is able to broaden its base of power and spread its reach deep into the liberal, Western democracies.

Paradoxically, the Western coalition’s attacks in Syria and Iraq are akin to extinguishing a fire with gasoline. The pictures and videos transmitted from the battlefields in Syria and Iraq and distributed on social networks will shift Islamic State sympathizers from frustration to action. Since the struggle depends on perceived injustice and discrimination and Western intervention is seen as motivated by economic interest, it is not hard for the Islamic State to rationalize the struggle against external infiltrators as a religious and national imperative.

Today, the response to the threat posed by the Islamic State is reactionary, minimalistic, and lacks any positive objectives for a desired future. It is only designed to prevent the enemy from achieving its aims. While there is no magic solution to defeating the Islamic State, the West must develop a long-term strategic rationale that incorporates simultaneous and synergetic action in all three circles of influence in which ISIL is trying to spread. This strategy must avoid the failures of Western policy in the Global War on Terror following September 11, 2011 and seek out a stable political settlement in the Middle East.

The West cannot rely on combating the Islamic State, mainly via air strikes, in the first circle of influence, in Iraq and Syria. A strategy centered on a military campaign ignores the importance of the Islamic State’s cyber and network presence in the second and third
circles. The West must develop new methods of warfare in order to be capable of dealing with the new types of challenges in cyberspace.

Furthermore, a relevant response demands an understanding of the implications of the cyber phenomenon at home and demands a variety of advanced tools and renewed thinking about laws and regulations. Just as Hamas fires at Israel from civilian population centers to cynically exploit Israel’s commitment to international law and morality, so too the Islamic State exploits Western norms of freedom and open expression to deploy cyber warfare against Western society. The West must find new ways to protect these norms while combating the organizations that exploit them.

Conclusion

The Islamic State’s activities in cyberspace, and in particular its computer network influence activity in social networks, demonstrate its broad potential for influencing societies and changing national and international agendas. Traditionally, cyberspace has been conceived as a realm of espionage and sabotage. The Islamic State has highlighted that cyberspace remains a potent area for influencing human action beyond the computer or cell phone screen, particularly among the younger generations. The Islamic State cleverly exploits the Western, democratic principles of freedom of expression, and has successfully instilled fear in the hearts of Western leaders to justify war against the terror group.

The post-Wikileaks revelations era presents new challenges for the intelligence community as liberal democracies demand greater protections for freedom of expression, privacy and respect for human rights. In May 2014, Stewart Baker, former general counsel at the NSA and former Assistant Secretary for Policy at the Department of Homeland Security, warned that in the wake of the Wikileaks revelations, intelligence organizations will enter a period of stagnation in the development of aggressive methods of information gathering. He fears that the West will lose intelligence capabilities without even being aware of the effect of their loss until it's too late.

Baker foresaw the situation accurately. It appears that the American response to the Islamic State will turn out to be a double-edged sword and will ultimately strengthen the terror group. The
Islamic State presents the Western coalition as a “crusade” against Islam that signifies the beginning of the end times. The Islamic State’s propaganda machine is well prepared for the West’s expected military response and has predictably called on its supporters worldwide to take Western military, police and politicians. Thus, it should be no surprise that we have witnessed a wave of terror against uniformed personnel and government institutions in the West.

Exactly a decade ago, the 9/11 Commission in the United States published its main findings. First, the government – from the president to the intelligence agencies – failed to think creatively. Second, the United States lacked organized policy. Third, the government failed to respond to emerging threats. And fourth, the government did not manage crisis efficiently. Ten years later, faced with a dramatic development of the same global threat, global jihad, the American-led West faces a similarly hopeless situation.

Today, the West’s preoccupation with cyberspace and cyber security focuses on espionage and attacks on critical national infrastructure. Terror organizations such as the Islamic State have no interest nor real ability to develop the ability to carry out cyber attacks of this sort. But, unlike Al Qaeda, which spent approximately a billion dollars to carry out the 9/11 attacks, the Islamic State found effective and inexpensive tools in cyberspace to strike at the West and fundamentally shift American foreign policy. As a result of the Islamic State’s cyber activity, the US president sent American forces back to Iraq and is now actively seeking to compromise with Iran over its nuclear program in order to build support against the Islamic State. The potential impact of computer network influence warfare and the difficulty in coping with it require significant R&D investment and the speedy adaptation of concepts and doctrines.

In the Israeli context, there is no guarantee that lessons from the Islamic States campaigns will not find their way to Hezbollah, Hamas, and other actors in the region. Israel has already experienced cyber attacks. At the beginning of 2012, at the same time as the establishment of the National Cyber Bureau in the Prime Minister’s Office, a Saudi hacker named 0xOmar reportedly stole credit card details of tens of thousands of Israelis. In an interview 0xOmar
stated, “Israel attacks and kills innocent Palestinians, it is carrying out genocide, and violates international law. The whole world has problems with Israel...I want to harm Israel financially and socially.” Hamas also tried primitive attempts to employ psychological warfare through technical means during Operations Pillar of Defense and Protective Edge. The Israeli Cyber Authority must ensure, as soon as possible, that the State of Israel and its citizens are capable of defending themselves against both traditional cyber threats and those only emerging today.

“OH, East is East and West is West, and never the twain shall meet, Till Earth and Sky stand presently at God's great Judgment Seat; But there is neither East, nor West, Border, nor Breed, nor Birth, When two strong men stand face to face, tho' they come from the ends of the earth!”

_Rudyard Kipling_
Bibliography


