INSS Insight No. 601, September 4, 2014

Cyberspace in the Service of ISIS

Tal Koren and Gabi Siboni

It is quite ironic that Hizbollah Secretary General Hassan Nasrallah, in an interview with Lebanese newspaper *al-Akhbar*, said that except for Israel, the Islamic State of Iraq and Syria (ISIS, otherwise known as the Islamic State) currently constitutes the most significant threat to stability in the region. Recent achievements by ISIS and the concern it arouses are highly evident in statements by various world leaders, including President Barack Obama, who said last week that the United States did not yet have a strategy for dealing with the organization, and Saudi Arabian King Abdullah, who warned that ISIS would turn its attention first to Europe, and a month later to the US. In truth, however, not much is known about the organization, because it has no centralized control, and its size and command structure, along with the identity of its leaders, are unclear.

Nonetheless, it is already obvious we are only at the beginning of a new fierce war in cyberspace. Indeed, while embodying the evil spirit of fanaticism, the organization's activity demonstrates the duality between what appears to be primitivism and 21st century cyber warfare. In turn, in a step that aroused much criticism, organizations affiliated with Anonymous announced late last week a full scale cyber war against the Islamic State (Operation Ice ISIS), intended to attack ISIS supporters using social media for propaganda purposes.

Hizbollah, Hamas, and al-Qaeda, as well as other jihad groups including ISIS, are well aware of the immense power of the social media (Twitter, Facebook, YouTube, and others) as an effective tool for distributing propaganda and political messages. These and other traditional media join behind the scenes activity designed to promote organizational ideology and recruit new operatives and resources. In contrast to the other groups, however, and as part of the doctrine it has adopted, ISIS resorts openly to a strategic deployment marked by sophisticated exploitation of the social networks on a previously unknown scale. ISIS's technological expertise evidenced thus far exceeds that of al-Qaeda and other jihad movements. The brutal execution of James Foley by a jihad operative with a British accent is no more graphic than other clips documenting the murder of other captives, e.g., Daniel Pearl. However, the viral dissemination of this clip

and others – most recently the beheading of Steven Sotloff – at an unprecedented rate by manipulation of Twitter and Facebook accounts and other applications that can be purchased from Google Store such as Dawn of Glad Tidings distinguishes ISIS from other organizations, and illustrates that another dimension of warfare combining physical and cybernetic jihad has appeared. A good example is that apparent executioner "John of the Beatles," the leader of a British gang operating in the ISIS framework, is quite possibly Abu Hussain al-Britani, a 20 year-old hacker convicted in 2012 for stealing information from former British Prime Minister Tony Blair and suspected of organizing complex cyber attacks against banks in the UK.

ISIS's main effort to date in cyberspace has focused on psychological warfare by generating fear through flooding the internet with video clips portraying the brutal acts of beheading and mass executions, as well as victory parades, as part of developing deterrence and creating an illusion of force in excess of the organization's actual strength. The essence of its online activity, however, is broader. It enables its supporters to obtain operational information, including training in preparing explosives and car bombs, and religious rulings legitimizing massacres in regions under ISIS control. In tandem, it distributes indoctrination materials, such as a magazine called *Dabiq: The Return of Khilafah*, which focuses mainly on topics relating to formation of the new Islamic state headed by ISIS leader Abu Bakr al-Baghdadi. However, ISIS's technological expertise is not the only factor. Perhaps the public, which is revolted by the organization's deeds but closely follows these clips and photos as a kind of reality show, is contributing a great deal to the organization's popularity.

While not much is known about ISIS offensive cyber activities, several indicators suggest that the organization has advanced capabilities in this field. First of all, ISIS, which several months ago split off from its former affiliate al-Qaeda, is led by a group of radical young leaders aware of the cyber capabilities and experience accumulated by al-Qaeda (e.g., transmission of encoded messages, religious rulings, instruction for preparation of explosives and car bombs), but with a greater understanding of technology. Second, as discussed in a special report that was published in London in 2012, leaking of advanced technological information from Iran and its ally North Korea to terrorist organizations is possible. Third, ISIS has an estimated $2 billion in assets from sales of oil, gas, and plunder (the bank in Mosul), enabling it to finance cyber terrorism while establishing links with international terrorist organizations. Fourth, a few months ago, groups affiliated with ISIS took control of the Twitter account of Anonymous using techniques similar to those used by hackers from the Syrian Electronic Army (SEA), an organization affiliated with the Assad regime, thereby demonstrating their high level of sophistication. Fifth, analyses published last month by IntelCrawler, a US intelligence company, indicate a dramatic rise in the use of malicious code (njRAT) around four main cities – Baghdad,

Erbil, Basra, and Mosul – apparently related to ISIS. Sixth, parties linked to the ISIS Electronic Army have made statements about carrying out a cybernetic jihad.

There is a cat and mouse dynamic on the internet comprising countries and activist international parties (such as Anonymous) aimed at inflicting direct damage on ISIS and its ability to raise online donations and disseminate its propaganda. Accounts of ISIS supporters are being suspended or closed. For their part, ISIS members are trying to evade such measures by activating existing accounts or opening new ones in place of those that were closed. Some of its activity has been moved to a different social network, Diaspora. Parties identified with Anonymous are also planning to attack countries they believe are financing ISIS (Qatar, Saudi Arabia, and Turkey) as part of a campaign (NO2ISIS), explaining, "We are unable to target ISIS because they predominately fight on the ground, but we can go after the people or states who fund them." Iran, which also has proven advanced cyber capabilities, will likely try to attack these countries, and there will presumably be more attacks such as the attack on the computers of the Saudi Arabian oil company Aramco.

The West in general and Israel in particular must consider how to strike the right balance between technology and the human element in intelligence gathering regarding organizations such as ISIS. Leaders must encourage cooperation between technology experts, social networks, and language experts capable of dealing successfully with the complex and changing reality. The effect of modern information technologies since 2009 (the Twitter revolution) on leaders of the political processes in many countries around the world (Ukraine, Moldavia) and in the Middle East, site of the Arab Spring (Egypt, Libya, Syria, Tunisia, and Iran) is stronger and more complicated than it appears. Without a successful concerted cyber-based effort, the "weapon of democracy" is liable to operate against its proponents.