***e-Info Ops*:**
Fighting terrorism with cyber ideas

*CDA Institute guest contributor **Eric Dion**, a doctoral student and former member of the Canadian Armed Forces, looks at the cyber dimension in the campaign against Daesh (the Islamic State).*

In an interesting twist in the so-called **«war on terror» against the Islamic State** (IS), also known as Daesh, a faction of Anonymous called the GhostSec is currently carrying out a cyber campaign called **#OpISIS**, targeting Daesh members and supporters who spread propaganda over the internet. There are also troubling allegations that Daesh is looking at literally acquiring, thanks to its own revenues, the capacity to conduct cyberwar, using the Dark Web for more than mere propaganda and recruiting purposes. Thus, beyond the conduct of Info Ops (**Information Operations**), Daesh is now looking at Cyber Warfare. In order to address this threat, a more integrated ***Comprehensive Approach*** is required, one which includes pro-active and positive Info Ops and an offensive Cyber Ops campaign.

The struggle to dominate the adversary in the battlespace in terms of information and intelligence can be traced as far back as Sun Tzu, who wrote: «To subdue the enemy without fighting is the acme of skill.» In this vein, Information Operations, including **Psychological Operations**, play an essential role. **Using the term Daesh instead of IS**, for example, is a simple way of negatively portraying the group, without the actual recognition given by employing the words Islamic and State together; such strategic messaging is not negligible, resulting in a pervasive effect over time. A good strategic Info Ops campaign would help determine similar elements to fight the terrorist rhetoric coming from Daesh as well as other extremist rhetoric. Indeed, in the current battlespace,

eric.dion@hec.ca

terrorism poses the most immediate threat, even if not an existential threat to Canada, our national interests, or values. As **I have said before**: We are not talking about a global cancer, but rather a wart.

One of the major issues currently underlying our Info Ops is the fact that **American laws hinder the cyber war** against Daesh: «Intelligence officials say that, as of mid-2015, ISIL almost exclusively uses US-hosted websites as its main channel of communications, propaganda and recruitment.» In many jurisdictions outside the United States, actions can be taken with relative legal ease to remove Daesh propaganda and limit its messaging capabilities. But the Fourth Amendment prevents US authorities from taking a more systemic approach to fighting Daesh online.

In Canada, those who use the Internet for extremist and terrorist purposes, either supporting the cause or more directly involved in messaging and communicating, can be arrested and prosecuted expediently. This was the case of the so-called **terrorist from Maskinongé in Québec**, who was sentenced to life for plotting online to travel to Egypt for a mission involving a bomb attack in Europe. He was also heavily engaged in online conversations and produced videos praising extremist attacks as well as distributing ransom demands for hostages.

Thus a ***glocal* (global and local)** strategy is needed. Taking a Comprehensive Approach, we should seek to establish a collaborative but glocally synchronised Info Ops campaign against Daesh, in order to continually disrupt their online outlets of terror. For example, Daesh's English magazine, titled «*Dabiq: The Return of Khilafah*,» has often been referenced by the media, such as **in the case of the bombing of Russian Metrojet flight 9268** on 31 October 2015 near Sharm el-Sheikh, Egypt. Such references give credit to Daesh's publication, and have a net effect of reinforcing Daesh's propaganda machine and online campaign. In actuality, such information should be discredited, not cited in the general media; it should be left for experts to analyze and for specialized information operators to disrupt.

Moreover, leveraging our Information Operations capabilities, we should see pro-active and even pre-emptive use of **Cyber Ops**, in a surgical fashion, against Daesh. Disrupting and virtually destroying its messaging capabilities should be combined with other Psychological Operations capabilities to affect Daesh messaging glocally, bringing forth a more nuanced view of the world. Indeed, we should be virtually fighting these extremist Salafi jihadists and their online brand of nihilistic violence by systematically shutting down there propaganda outlets and social networks, if these networks don't do it on their own initiative. What's more, we should limit the media coverage of terrorist events to a bare minimum. Such Info Ops campaign should thus be part of a concerted **Comprehensive Approach**.

Sheer terror on the part of Daesh has only been reinforced by the west's 24/7 media and social networks, which inadvertently spread Daesh's message by hosting them online. In the case of the Paris attacks, we have come to know more on the part of the terrorists than on the part of the people who were lost or wounded; it is their stories of courage and

humanity in the face of terror which should be the key messages. Indeed, any good strategic communications campaign would obviously rule out any form of messaging on the part of Daesh in any medium, while also however emphasizing their atrocities and their crimes against humanity. The effort and the scale of the air bombing campaign should also be put into a well-orchestrated and positive information operation on a glocal scale to **Countering Violent Extremism (CVE)**, obviously including Daesh. Psychological Operations should be carried out in a surgical cyber fashion, as much as Special Operations carried out on the ground to «cut-off the snake's head».

More concerning however, is also the fact that Daesh is seeking to acquire capabilities in order to conduct **Cyber Warfare**. Such potential capabilities to damage our own critical information infrastructure – like in the finance, energy, communications, or government sectors – poses the risk that the Dark Web, as it is called, becomes a literal battlespace. Thus, according to **War on the Rocks**: We should employ «offensive technical measures against Daesh social media networks, better monitoring the group's efforts to recruit or rent skilled hackers via the Dark Web, and the intelligence sharing necessary for the identification and arrest of hackers either sympathetic to or cooperating with Daesh». Deliberately attacking these virtual mediums should be part of a **Cyber strategy**.

Although perhaps well intended, uncoordinated actions by groups like Anonymous pose the risk of jeopardizing the intelligence agencies› access to online information on Daesh and its supporters. Conversely, a more integrated Comprehensive Approach in tackling terrorist propaganda would seek to fight extremists with cyber ideas, and not simply by virtually shutting down our eyes. We should consider online radicalization as a key precursor for extremism and terrorism. We should be leveraging Info and Cyber Ops against Daesh, fighting terrorism with ideas online, and **reducing to nil their own nihilistic thinking**.

We need to employ a Comprehensive Approach that combines all of the tools of national power, including Info Ops and Cyber Ops to treat symptoms, as well as the disease itself. **«Another dimension of warfare combining physical and cybernetic jihad has appeared.»** A military response is just one piece of the puzzle. We also need to counter the pressures of alienation within society and fight all forms of extremism, namely against Muslims, that is abroad or within our own communities and jurisdictions. We need to be providing our military, police, and security forces with the framework that allows them to conduct pro-active and positive Info Ops, as well as offensive and pre-emptive Cyber Ops. Indeed, **Daesh may be more dangerous than ever**, but we should simply be smarter.

Eric Dion *is a doctoral candidate in management who is also retired from the Canadian Forces. (Image couresty of Wikimedia Commons.)*