Nigel Somerville discusses the importance of open source intelligence gathering in countering the growing terrorist threat to critical infrastructure

OPEN SOURCE

©Getty Images

©Getty Images

Terrorist groups today are relying more and moreon modern technology to facilitate their objectives. Global and decentralised in nature, extremist groups are now exploiting the Internet, mobile phones, social media and widely available software with a sophistication never witnessed before. They are leveraging this technology with a truly entrepreneurial spirit. This is revolutionising propaganda, recruitment, training, fundraising, communication, and targeting.

Until recently, al-Qaeda and its affiliates regarded the Internet as an opaque place to disseminate material anonymously or meet in "dark" spaces. The traditional method of releasing information involved password-protected forums, the use of proxies to hide Internet Protocol addresses to prevent tracing, and access was restricted to use by a computer.

By contrast, recent extremist groups such as ISIS have modernised their approach. They now embrace the web as a bright portal in which to promote themselves, intimidate people and radicalise new recruits. They display brazen proactivity in the use of mobile devices, social media and the interactive capabilities of the Internet to their full potential. Instead of waiting for users to happen across their websites and propaganda, terrorists now actively lure targeted individuals and groups to their pages. Online grooming is then used to create an emotional, psychological or intellectual bond to generate support for the cause. This is then reinforced by the sense of community and that an online grouping can provide.

These modern factions use Twitter, Facebook and WhatsApp and, vitally, a language common to peers. ISIS is a leading example of this modern approach, and is believed to have up to 50,000 different Twitter accounts tweeting up to 100,000 messages a day. It treats media with a professionalism hitherto unseen among extremist groups. Videos have a self-conscious online gaming quality, utilising exaggerated effects and features. Furthermore, trending Twitter topics like "World Cup" and "Ebola" are hijacked to insert ISIS messaging into wider news feeds. This hashtag-hijacking is complemented by a startling capacity for volume and effectiveness, as exemplified by ISIS issuing 40,000 tweets a day during the advance on Mosul without triggering spam controls.

Other organisations are following the trend. Hamas, Hezbollah and the Syrian al-Qaeda branch, al-Nusra Front, are all now using Twitter. On 14 January, the al-Qaeda branch in Yemen claimed responsibility via Twitter for the Charlie Hebdo attacks in Paris that killed 17 people. The group has two official accounts on Twitter and their activity looks set to increase.

Online platforms are also used for basic planning and logistics. Web forums such as those used by al-Ansar, an al-Qaeda affiliate group, act as a "matchmaking service" to co-ordinate new militants for the front lines in Iraq. Paltalk, a voice and video chat room, was a strong connector for people during the Arab Spring. The men who plotted to bomb the London Stock Exchange allegedly relied heavily on the service. Insecure email groups such as Yahoo eGroups are also common. Meanwhile Twitter, Ask.FM and to some extent Facebook, have all been used to plan and co-ordinate activities and ideas. Recent topics relating to Syria that have been common include how to change money, where to get mobile phones, how to travel securely and how to minimise Islamic profiles when under the glare of transport security.

Previously it was relatively simple to use data-mining tools to monitor this open-source activity. Sadly, the modern reality is that the monitoring landscape has fundamentally changed post-Snowden due to the leaks' exposure of intelligence-gathering techniques and capabilities. As a consequence, extremists now routinely employ readily accessible software and encryption services to communicate their sensitive and critical information. This allows them to communicate instantly and securely around the globe, retreating from the open and insecure realms of social media.

In the post-Snowdon environment, open-source intelligence gathering in the UK is more likely to benefit terrorists than intelligence services

Groups encrypt emails, web boards and social networking sites through services like PGP (Pretty Good Privacy) or homespun organic variants such as al-Qaeda's Mujahideen Secrets. Meanwhile, voice communications can be encrypted with systems like PGPfone, Zfone and ZRTP. Commercially designed, these services prevent "man-in-the-middle" wiretapping attacks and provide a voice communication encryption capability equivalent to a STU-III, the US government's highest level of encrypted secure telephone capability.

This encryption has therefore changed the very nature of counter-terrorism work. We can no longer rely on previously enjoyed levels of communication monitoring. The consequence today is that intelligence revelations are rarely likely to come through open source social media. The reality is that national security intelligence breakthroughs are now likely to be limited to an occasional mishap with Twitter's geo-tagging functionality.

The security and intelligence communities therefore need greater support from the private sector to address this issue – particularly from the large US technology companies who provide these web services. To some, these corporations are even seen as facilitators for insurgent activity, providing the command-and-control networks of choice. If security agencies are to meet this new security challenge at scale, it means navigating the complex environment of privacy laws to allow thorough (but acceptable) legal investigation.

Due to the paradigm shift in how we now produce and store data, the web offers unprecedented open source intelligence opportunity for extremists. This open source intelligence, derived from publicly available sources of information is not a new phenomenon. As Tsar Nicholas II proclaimed during the Crimean War, "We have no need of spies. We have the Times of London." What is new and significant, however, is the sheer volume, variety and value of the information available. In 2000, 25 per cent of the world's information was stored digitally. Today this is more than 98 per cent. This shift in data habits offers unprecedented opportunity for those who want to exploit it.

So what for tomorrow? The future threat will be defined by hyper-connectivity and cybercrime. We are heading towards interaction, communication and collaboration between people, devices and places on a scale never imagined before. Already, we are some way down this technological super-highway. Experts estimate that, during 2015, there will be 25 billion connected devices and, by 2020, 50 billion.

Components of infrastructure and corporate real estate that stand to benefit most from hyper-connectivity will also be the most vulnerable. The Internet of Things will prevail and "smart" buildings will become governed by systems, sensors, networks and devices all inter-connected to improve efficiency by remote or automated control. In consequence, they will also therefore be the most vulnerable to remote attack as these sensors, networks and devices inherently lack suitable security or protection.

While these systems represent the brain and nerves of future infrastructure, the security risks have never really been considered in the modern hyper-connected environment. In fact, many of the devices and sensors used in modern buildings will never have had security incorporated into their design. It is also not always clear where security responsibility lies, as the threat spreads across corporate functions including IT, physical security, technology and facilities management. The HR function is also an increasingly critical component, since people often represent the weakest link of the security chain and the use of social engineering by terrorist groups is a growing concern.

We are already seeing these systems come under threat. In June 2010, the Stuxnet 500-kilobyte computer worm proved that cyber crime can inflict physical damage. At least 14 industrial sites in Iran, including an uranium-enrichment plant, were physically affected by cyber attack. Chevron then became the first US corporation to admit that Stuxnet had spread across its machines. In 2013, the Associated Press was hacked by the Syrian Electronic Army leading to a news alert announcing an explosion at the White House and the injuring of President Obama. This may have cost the stock market as much as $136 billion. What was essentially an act of vandalism had the impact of a terrorist attack.

In October 2012, US Defense Secretary Leon Panetta warned that the United States was vulnerable to a "cyber Pearl Harbor" that could derail trains, poison water supplies and cripple power grids. Why target a highly secure military facility when you can knock over public power utilities, critical national infrastructure, a city's supply distribution networks or the banking system? If money is the sinew of war, what happens if the financial system is crippled? Future cyber and terrorist attacks could therefore directly impact civilian workplaces, individuals and business operations. There could be physical or virtual damage inflicted to equipment remotely.

We are already seeing a classic arms race. The Cold War has become the "Coders War". We are advancing aggressive cyber capabilities but feeling less and less secure. Most sophisticated cyber weapons are being designed to inflict damage. Real, physical damage. These weapons are bespoke, expensive to build, and have a very short shelf life. What is also remarkable is that unlike the well-understood laws of armed conflict, no one currently knows what the rules of cyberwarfare are. This falls into the sweet spot of terrorism.

As cyberterrorism becomes more of a reality, the home front will become more of an unexpected battlefield. Modern corporate competitive advantage will be increasingly driven by volume and usage of "fast data" – that is, data which is collected and analysed in real time to support real-time decision processes. This provides early warning systems based on opinion mining and real-time awareness feedback. As well as physical threats, we can also therefore expect to see new forms of blackmailing and extortion schemes such as "ransomware" for data theft, or disruption of smart machines, smart offices or buildings.

The modern security environment is shifting rapidly. Threats are ever-changing and the blend between physical and cyber threats is advancing. All employees and functional areas are equally vulnerable. Understanding the threat and investing in appropriate security will be essential from the outset, as will board-level responsibility for ensuring it. This will not be easy. We will need to see collaboration between individuals, businesses and government; otherwise we risk leaving ourselves vulnerable and exposed.

Nigel Somerville MBE MC leads the international Risk Management function at Source8, following 17 years of operational and strategic national security roles in the UK military. He has significant experience in conducting highly challenging and strategic programs worldwide, with expertise in risk management, business intelligence, information and physical security, corporate due diligence and commercial compliance.

More co-operation is needed between the large US technology companies and the intelligence agencies to exploit open-source intelligence

©Getty Images