EXPERT CONTRIBUTIONS

EXPERT CONTRIBUTIONS

Cyberterrorism is the New Frontier

SERGE STROOBANTS, DIRECTOR OF OPERATIONS FOR EUROPE AND MENA, INSTITUTE FOR ECONOMICS AND PEACE

Europe has been thrust into the epicentre of the recent evolution of terrorism, with France, ranked 30th on the 2017 Global Terrorism Index, reflected in its exposure to novel attacks in recent years. France is one of the highest ranked countries on the index not directly involved in an armed conflict, which is the foremost driver of terrorism. It is ranked so high because it had been exposed to many first time attacks in the recent years: guerilla tactics, urban warfare, suicide bombers in Paris, and a lorry attack in Nice show a society and its security services untested and maladapted in covering vulnerabilities emanating from new threats of terrorism. Coupled with this was the hybridisation of terrorism and the cyber world, effectively weaponising propaganda and ideology, spreading extremist belief, facilitating recruitment and radicalisation, but also galvanising and directly prompting terrorist attacks.

Such was the case for the beheading of a French priest in Normandy in July 2016, where the perpetrators were not only radicalised online, but received their directives and were ordered to their respective assignments via mobile networks. This follows a greater trend, noted by the Financial Action Task Force in 2015: the internet is the most commonly used tool for recruitment as well as support for terrorist organisations.

While internal security services have responded to these terrorist attacks and events with assistance from military and intelligence units, terrorist organisations found a vulnerability which lies at the blurred border of internal and external security. Within this grey area between terrorism and insurgency, between conventional and unconventional techniques and targets, between the real and the virtual world, it is extremely difficult to come up with the right prevention and the right response.

Syria has been a trial by fire with regards to the nascence of the "remote command and control". Many European terror plots were not only planned in Syria, but were directed in live-time from Syria via internet and encrypted internet communication platforms. Despite the general defeat of groups such as ISIL on the ground, which are unable to plan and execute directed attacks against European targets, homegrown terrorists remain a threat, especially as groups such as ISISLshift their focus from encouraging jihad by traveling to a region, and instead encourage followers to strike in their own countries.

This homegrown or lone-wolf terrorism can be inspired and controlled by external terrorist groups or operatives in the commission of their crimes, and state responses only develop following a first strike of this new type of attack. States should be proactive regarding cyberterrorism attacks, and should bring security back, particularly to Europe, by taking preventative measures by learning about available strategies, tools, and techniques regarding cyberterrorism. New wars should not be fought with the strategy of the previous one: cyberterrorism is the new frontier.

Cybersecurity is an emergent issue and focus for various states and organisations, commensurate with an increase in both awareness of cyber vulnerabilities, as well as noted exploitations, denial of service attacks, and malware. Due to the centrality of cyberspace to daily life, cyberattacks have become increasingly threatening, disruptive, and frequent.

Attacks on civilian utilities such as internet access, hospital systems and power grids have all occurred in the past years, from both state and non-state actors. The largest non-state attacks affected critical structures, such as the National Health System shutdown during the Wannacry attack of 2017. This undermines national and international security, can adversely affect critical infrastructure, and can thus threaten the safety of civilians, leading to the conception of cyberterrorism. Cyberterrorism is an attack against electronic infrastructure for a political purpose, or to cause and inspire fear in the general public through electronic means.

Cyberterrorism has been a known strategy since the leader of the Al-Qa'ida affiliated Jemaat Islamiyah dedicated a chapter in his extremist literature to attacking US computer networks due to their susceptibility to money laundering and credit card fraud. Also included was a roadmap of sorts, with connections to hacker mentors and

sites which explained how to successfully carry out such a cyberattack as well as conceal their identities. Infamously, IS has used the relative lawlessness of the cyber realm to perpetuate their form of terrorism. IS has mobilised terrorist cells, using encrypted messaging to plan, recruit, and carry out their attacks, with a new focus on "homegrown terrorism". This differentiates from their earlier strategy of encouraging supporters to travel directly to their conflict zones. IS has also participated in hacking, managing to hack into US Department of Defence databases, steal the information of military personnel, and publish this information as targets online, alongside detailed instruction manuals regarding homemade explosives and appeals for funding.

Terror organisations such as ISIL cannot exist without funding. Cyberterrorism plays a role here. One noteworthy Al-Qa'ida operative, tasked with publishing extremist and radicalising videos on the internet, had stolen over 30,000 credit card numbers, laundered the stolen money through online gambling portals, then transferred the laundered money to bank accounts used to purchase weapons for the terrorists and to support the organisation as a whole. This system of online credit card fraud was used to partially fund the 2005 London metro attacks, which shows the potential of this cyberterrorist nexus. The Al-Qa'ida operative, for instance, was able to use readily available tools to obscure his identity, including VPNs, proxies, and software to hide his IP address – even using US-based companies for the hosting of his terrorist propaganda.

Cyberattacks do not have to be so kinetic to inflict damage, nor do they have to be so lethal to harm or incite fear. Most cyberattacks being innocuously enough, with a simple phishing attack presented through an infected email attachment. The unsuspecting victim opens the attachment, which then downloads malicious code into the network, spreading to other computers on the network. This tactic was suspected to be behind the ISIS Cyber Caliphate takeover of the Central Command's twitter profile, where strategies and personnel names were leaked. Phishing gives the attacker access to the same data available to the user – financial information, classified or sensitive information, the performance of a critical system, or even access to water or electric grids.

Financial institutions have long been targets of terrorism, and this is true online as well. In the case of the 2016 Bangladesh bank heist, malicious program, likely malware sent through an email, was installed on the bank's computer system. The malware then collected passwords and usernames, and deleted evidence of its own presence, rendering it virtually invisible. These stolen credentials were then used to access SWIFT, the most secure global money transfer system. 81 million USD were lost in four transactions. One operative of Hizbut-Tahrir al-Islami similarly defrauded banks on a much smaller scale, running false or double transactions at his Russia-based café, then using these illicit gains to fund his terrorist group.

Distributed Denial of Service attacks, or DDoS attacks, are also popular, easily available, and inexpensive ways to disrupt civilian life. DDoS attacks involve overwhelming the bandwidth of an institution by flooding the institution's system with targeted and unrelenting communications and requests, which force the institution offline due to exceeding data capacity. This overload leaves the service or network unusable or inaccessible for the users. ISIS's Cyber Caliphate used these attacks successfully against Yemeni and Iraqi government sites in January 2017, forcing the sites offline for two months, until they emerged with new hosting – which included DDoS protection.

"Many European terror plots were not only planned in Syria, but were directed in live-time from Syria via internet and encrypted internet communication platforms."

Ransomware attacks are also popular methods which combine the disruption of a denial of service with an ability to gain profit by taking over an institution's network infrastructure, and holding it ransom, forcing the affected entity to pay a fee to regain control of and access to their systems. Europe experienced a widespread ransomware event in May 2017, when the Wannacry attack took place. This attack especially effected the UK, where hospitals were unable to access basic medical records, causing for cancelled appointments, surgeries, and lead to the shutdown of sixteen hospitals. In the United States, the city of Atlanta had first responders unable to use their databases, and citizen services were taken offline as unidentified hackers deployed ransomware, demanding $51,000 in Bitcoin to return control to the city.

Terrorism has emerged in cyberspace as a natural response to kinetic security responses and traditional military measures. International organisations have recognised this emergent war zone, as NATO recognised cyberspace as new battle environment, and an impetus for invoking collective defence at the 2016 Warsaw Summit. However, states generally pursue their own policies, and

international cooperation regarding cyberterrorism remains low. While the European Commission has recently directed the EU towards a single cybersecurity market with open communication between state entities, standards for certifying secure internet connections, and increasing intelligence sharing regarding cyberterrorism, there remains no global standardised approach to the cyberterrorism challenge. While both the United States and the United Kingdom have strong, well-funded institutions addressing specifically the issue of cyberterrorism, few other states are individually as prepared, and are attempting to address the challenge these cyber threats pose completely on their own.

The 2005 EU counterterrorism strategy focuses on four pillars: prevention, protection, pursuit, and response. Prevention aims to address the causes of radicalisation and terrorist recruitment. Protection emphasises defence of citizens and infrastructure, and reduction of vulnerability to attacks. This aims to secure external borders, improve transport security, protect strategic targets and reduce the vulnerability of critical infrastructure. Pursuit intends to hinder terrorist capacity to plan and organise attacks, as well as to bring perpetrators to justice. Response comprises the preparation for and the management and minimisation of the consequences of a terrorist attack through improving capabilities in dealing with the aftermath of a terrorist attack, the coordination of a response and to address the needs of the victims. This pillar is the most international, emphasising the need for EU solidarity through crisis coordination arrangements, revising civil protection mechanisms, integrating political crisis response arrangements and sharing best practices in assisting victims of terrorism.

Some major approaches to tackling cyberterrorism are partnerships with corporate entities and major leaders in the cyberspace field, to creating cyberspace bootcamps for the offensive and defensive training of servicemembers tasked with cybersecurity. Others focus on global governance, with nations increasing not only their information sharing, but their attempts to create a standard response protocol to these cyber terroristic incidents, such as the formation of a database of known extremist imagery to be share with internet protocol providers to automatically remove such images from the internet.

Another issue is the popularisation of the blockchain, a cryptographic peer-to-peer exchange protocol usually accompanying cyber cryptocurrency transactions which occur openly, with no oversight, no restriction, global manoeuvrability, and with near anonymity. For this reason, Bitcoin and other untraceable internet-based currencies have also become desirable and anonymous ways to fund terrorism and its activities. Transactions can be in the form of exchanges, cryptocurrency mining, and donations. The nature of the blockchain allows for the layering of funds, through purchases, electronic money transfers, of virtual currency accounts, giving the veneer of legitimacy, as well as obfuscating a trail already difficult to follow. The formation of front companies in purchasing cryptocurrencies in more regulated markets can avoid triggering reporting mechanisms and can further confuse legal and illegal income. Some large financial hubs have enacted laws around due diligence regarding cryptocurrency clientele, as well as identity verification procedures and mandatory reporting of suspicious transactions, but these countries are in the minority.

States need to regain the initiative in addressing cyberterrorism to maintain the advantage over terrorists and terror organisations who are hybridising their physical attacks with internet capabilities. Rather than waiting for the threat to become real and then responding to physical force of the attack, states should seek to avoid surprises to protect their citizens, as well as their interests. The confrontation between states and terrorists should be led by the state, with a would-be attack pre-empted by a strong, decisive plan or strike, which could serve as a deterrent. Stricter regulations on, and closer partnerships with companies which operate in cyberspace would help identify and prevent would-be terrorists, as well as better-trained personnel dedicated to handling cybersecurity and cyber threats. In this way, states will be able to recede from defensive strategies and instead deploy offensive ones, demonstrating their capabilities and securing a more peaceful nation overall.

“The 2005 EU counterterrorism strategy focuses on four pillars: prevention, protection, pursuit, and response.”