Articles

Islamic State and Technology – A Literature Review

by Truls Hallberg Tønnessen

Abstract

This article offers an overview of the literature on how the Islamic State has used different technologies, primarily within the fields of drone technology, CBRN and communication technology. The author argues that the primary strength of the Islamic State, and terrorist groups in general, is not in the acquisition and use of advanced technology, but the innovative and improvised use of less advanced, but easily accessible, technology. A gap identified in the existing research is the question of priority – why and under what circumstances would a terrorist group allocate some of its (usually) limited resources in order to develop or acquire new technological capabilities?

Keywords: Technology, Terrorism, Islamic State, CBRN, Drones, Internet.

Introduction

The aim of this article is to offer a brief overview of the literature on Islamic State (IS) and technology. The intention is to identify knowledge gaps within the literature and to make some preliminary observations on the Islamic State's use of specific technology.

Since it is somewhat difficult to separate the literature on technology and Islamic State from the more general literature on terrorism and technology, this article will, indirectly, also be a presentation of the larger literature on terrorism and technology. However, given the unprecedented scale of the Islamic State's territorial control, financial resources and the number of recruits, the Islamic State has, at least until its recent demise, been at the forefront of technological development among contemporary terrorist groups. In this overview, three fields of technology that have received most attention in the literature - drone technology, communication technology and CBRN – have been singled out. These fields are also some of the fields where the Islamic State has been most innovative. All of these technologies can be used as part of offensive operations.

One main argument made here is that while the general literature on terrorism and technology tends to focus on the most advanced and most lethal scenarios, the primary strength of terrorist groups is their innovative use of less advanced and easily accessible technology. The present study finds that, like most terrorist groups, the Islamic State has used some of this technology mainly for defensive purposes and when the group has used technology offensively, it has done so in a crude, improvised and "low-tech" manner. It is also argued that, although the Islamic State has been innovative in the use of technology and made technological improvements, this is mainly an effect of IS' ability and willingness to exploit new opportunities given by the rapid technological development and by the sheer size of the group. The primary gap in the literature identified in this review is the issue of priority – why and under what circumstances would a terrorist group allocate some of its (usually) limited resources in order to develop or acquire new technological capabilities?

General Observations on the Literature

The literature on terrorism and technology can generally be divided into two categories. On the one hand is what we may refer to as "what if" writings and scenario-oriented literature, looking mainly at which *capabilities* a non-state actor would require to engage in, for instance, a CBRN attack or in an act of cyber-terrorism, and the *probability* that a non-state actor would be able to acquire the resources and competence needed.[1] Given the (fortunate) rarity of incidents of CBRN attacks and acts of cyber-terrorism, this literature is often highly technical and theoretical.[2] This literature has at times been criticized for exaggerating the threat and the probability of highly advanced and potentially very lethal attacks.[3]

There has also been a tendency in some of this literature to conflate non-state actors with their limited resources with states that have developed highly advanced technology.[4] For advanced technological fields, like CBRN and cyber, it is undoubtedly states, and not non-state actors that represent the greatest threat, if they choose to use it offensively. However, it cannot be ruled out that non-state actors could directly or indirectly be given access to advanced technologies and resources by states that, for instance, want to avoid attribution.[5] Thus, a major caveat of this literature review is that it has not looked at the literature on technology and state-sponsored terrorism.

Another type of literature looks at terrorist organisations' *motivation* to use certain technologies. For instance, some of this literature discusses a non-state actor's motivation and various incentives and disincentives for the use of CBRN.[6] This literature is often more empirical –either based on actual incidents or focusing on statements of intent from terrorist groups or key individuals.[7] However, as this article will illustrate, it is often not enough to look at terrorist groups' stated intent. Intent does not equal capability, certainly not in technologically more advanced fields.

Islamic State and CBRN

There has been no shortage of politicians and security analysts warning that Islamic State (or other terrorist organisations) may use various forms of CBRN weapons, even nuclear weapons, for an attack.[8] And there is no doubt that the motivation to use CBRN weapons indeed is present – in 2014 it was estimated that there have been 50 registered incidents where al-Qaida or its affiliates have attempted to acquire, produce or deploy CBRN weapons during the last two decades.[9] There have also been a handful of incidents in Europe where CBRN materials have been considered in the planning phase of a terrorist attack.[10] However, the low number of actual incidents including CBRN indicates that ambition fortunately has so far exceeded capabilities. Jihadists' lack of competence and lack of development within the field of CBRN has been confirmed by a 2015 study based on the discussions of CBRN weapons and various CBRN "recipes" posted on online jihadist forums.[11]

Symptomatically, terrorist groups have so far primarily used the least advanced form of CBRN – chemical weapons. The University of Maryland's Global Terrorism Database (GTD) has registered 303 incidents of terrorist attacks including chemical weapons worldwide. In comparison, GTD has registered 32 incidents of biological terrorism worldwide, resulting in 9 fatalities, no incidents of nuclear terrorism, and 13 incidents of (attempted) radiological terrorism, resulting in no fatalities.[12] Of the al-Qaida affiliates, it is the Islamic State and its predecessors that have been regarded as the most successful in the development and use of chemical weapons.[13]. Al-Qaida's history of experimenting with, and using, chemical weapons goes back to the 1990s when Abu Musab al-Zarqawi, the Jordanian founder of al-Qaida in Iraq, established a camp for foreign fighters in Herat, Afghanistan.[14] In 2007 the Islamic State of Iraq, as the group was known at the time, was responsible for a series of attacks that combined truck bombs with canisters of chlorine. Many died as a result of the attacks, but apparently not due to the chlorine, but due to the conventional explosion itself.[15]

Following the establishment of the Islamic State in 2014, there was a rapid increase in the group's use of chemical weapons. According to an estimate by IHS Conflict Monitoring, the Islamic State is believed to have been responsible for 71 incidents of chemical attacks between July 2014 and June 2017.[16]

There are also indications that there has been an improvement in the Islamic State's chemical capabilities since 2014. This development was the result of what may be referred to as a chemical weapons program, including some veterans from Saddam Hussein's chemical weapons program.[17] For instance, the Islamic State has been able to manufacture shells filled with chemical agents and successfully delivered them over a greater distance, using mortar grenades. Chlorine was still the most frequently used chemical, but IS has also succeeded in both manufacturing and weaponising mustard gas.[18] This is a worrisome development that should raise some concerns. However, so far few incidents attributed to IS have been reported where the chemicals alone have caused causalities. The impact of the Islamic State's use of chemical weapons has thus far primarily been psychological, not physical.

Taking into account the group's access to substantial financial resources, its vast pool of recruits, its territorial control and the group's long history of experimenting with chemical weapons, it is rather surprising that the group's capabilities did not evolve more than they did. As pointed out by Geoffrey Chapman elsewhere in this Special Issue, what characterizes the Islamic State's use of chemical weapons is the scale of its use, not its technological sophistication.[19] So far, concerns that IS should acquire more weapons-grade and more advanced chemical weapons, such as sarin, from the stock-piles of the Syrian regime appear to have been unfounded. IS has primarily used crude and improvised chemical weapons and most reports point to the Syrian regime as the culprit behind sarin attacks in Syria.[20]

There have also been concerns that IS could succeed in weaponising other forms of CBRN materials than chemicals, such as radiological substances building a radiological dispersal device (RDD) or "dirty bomb". The Islamic State had access to various sources of radioactive material in Iraq, particularly in Mosul's hospitals and university institutes. This has led to concerns that the group could be able to develop an RDD.[21] However, experts have concluded that the radiological material IS had access to had limited utility for constructing a dirty bomb.[22] There have also been concerns voiced that the Islamic State could be able to buy some sort of nuclear device or materials on the black market.[23]

An article published in Islamic State's magazine *Dabiq* alluded to the fact that IS might be able to use its unprecedented access to financial resources to obtain a nuclear device from Pakistan and smuggle it to the United States and detonate it there. The author of the article admits that this might be a far-fetched scenario, but that the scenario nevertheless would be the "sum of all fears of Western intelligence agencies".[24] In addition, the possibility that a state in possession of nuclear weapons, like, for instance, Pakistan, should willingly sell a nuclear device to a non-state actor has been discredited.[25]

However, an incident in Belgium illustrates the typical "low-tech" and asymmetrical threat that IS, and other terrorist organizations, may represent. Members of the IS-linked attack cell that was responsible for the attacks in Paris November 2015 and in Brussels in March 2016 had been spotted on several hours of video surveillance footage targeting a Belgian nuclear scientist working at a nuclear research center. One police theory is that the cell planned to abduct him and force him to provide them access to radiological materials.[26] The same cell reportedly also planned mixing certain animal excrements with explosives to construct a primitive "biological weapon."[27] Additionally, a Belgian recruit of Moroccan origin, who used to work at a nuclear power plant before travelling to Syria, illustrates the potential of insider threats.[28]

Islamic State and Drone Technology

The Islamic State has made their most technological progress in the field of drone technology.[29] One of the most comprehensive reports on terrorist groups' use of drones, published in 2016, identifies four groups with discernable "drone programs" – Hizballah, Hamas, Islamic State and Jabhat Fatah al-Sham (formerly known as Jabhat al-Nusra). Tellingly, all four had territorial control to varying degrees and three of them have been involved in the ongoing conflict in Syria.[30] Hizballah and Hamas were pioneers when it came to exploiting the possibilities offered by drone technology, but the rapid development of the drone program of the Islamic State is striking. According to the report, it took approximately seven years from Hizballah demonstrating some interest in drone technology until the successful use of a drone as part of an operation, while the same trajectory took only about one year for the Islamic State.[31] This rapid development is even more striking, knowing that Hizballah received some support from Iran, while the Islamic State did not enjoy such state support.[32] A partial explanation is that the rise of the Islamic State coincided with a rapid development of the availability and commercialisation of drone technology.

The Islamic State primarily used commercially available drones that were modified for military use but also experimented with constructing simple surveillance drones 'in-house'. Conflict Armament Research has identified several IS-drone workshops, for instance in Ramadi and in Mosul, where IS modified and weaponized drones and also manufactured some from scratch.[33]

The Islamic State initially used drones for surveillance and for propaganda purposes, but there has been a rapid increase of weaponised drones. In September and October 2016 it was reported that the Islamic State had managed to weaponise drones by attaching explosives that could be released when the drone hovered over an intended target.[34] In October 2016 two Kurdish Peshmerga soldiers were killed and two French Special Forces badly injured in what has been described as the first confirmed incident causing casualties following a terrorist organization's use of a weaponised drone. This incident also illustrates the unconventional and innovative offensive use of drones by the Islamic State. The drone in question was brought down to a landing without any casualties, but it had been rigged with explosives that blew up when the Kurdish Peshmerga soldiers were inspecting the drone. [35]

There was a rapid increase in reports on the Islamic State's use of weaponised drones after the group announced the establishment of a separate drone unit in January 2017. According to a publication by the IS-affiliated al-Yaqin foundation, the Islamic State's drones succeeded in killing 39 persons and destroying 43 vehicles in February 2017 alone.[36] Thes numbers are probably exaggerations ,but there has been a steady uptick of deadly drone attacks. In September 2017, media reported that a dozen Iraqi soldiers had been killed by Islamic State drones.[37]

This rapid development seems to have been the result of a concentrated effort by IS to develop a drone program. The existence of such a drone program was confirmed by the discovery of the so-called "drone papers" in Mosul in 2016. Most of the documents found were produced in 2015; – these papers indicated that IS had, at least to some extent, developed a streamlined and bureaucratised program for development and weaponisation of drones. Several of the documents pertaining to acquisition of drone parts were signed by the Aviation section (*qism al-tayaran*) of the group's Committee of Military Manufacturing and Development (*Hai'a al-tatwir w al-tasni` al-`askari*). The existence of a specific committee for military manufacturing and development illustrates that this was something the group prioritised.[38] A 2017 report, based on information obtained from several local sources based in Syria, illustrates the extent of the group's drone program. The report identified separate centers for training, weaponisation, modification and maintenance, as well as the existence of a center for storage and distribution. Each of these centers had its own director, and all were based in Raqqa. The overall leader (or emir) of the Islamic State's drone program was identified to be a Muhammad Islam, a European citizen of Malaysian descent who holds a degree in information technology from a British university.[39]

Although the Islamic State has made rapid improvements in the use and weaponisation of drones, it can be argued that drone technology in itself has worked against the Islamic State since many of its top leaders have been killed by the technologically much more advanced U.S drones. For instance, by March 2016 it was estimated that 90 senior and mid-level IS leaders had been killed by drone strikes.[40] This supports the general observation that technology, especially more advanced technology, often works to the disadvantage rather than the advantage for non-state actors.

In addition, there are a number of anti-drone measures that might reduce the threat from non-state actors' use of drones. For instance, through use of geo-fencing, DJI, the producer of the most popular commercial drones, has prevented its models from flying in parts of IS-controlled areas in northern Syria and Iraq.[41] The U.S-led Coalition Forces in Iraq have also used several anti-drone tools against the drones of the Islamic State, such as the anti-drone rifle Battelle DroneDefener and one called Dronebuster.[42] This illustrates that although non-state actors start using more advanced technology, their opponents still stay ahead of the curve because states are more capable of rapid technological development than non-state actors are. However, the rapid commercialisation of drone technology has contributed to reducing this gap - a development likely to continue.[43]

Islamic State and the Internet

The literature on Islamic State and the Internet falls mainly in two categories. The first category is literature focusing on how the group has taken advantage of the opportunities provided by the Internet and especially by social media, for instance in the fields of recruitment and dissemination of propaganda.[44] A large part of this literature focuses on the actual content of the propaganda and not on the Islamic State's use of internet technology per se.[45] The second category is of a more technical nature and focuses on the online infrastructure of the Islamic State - such as which platforms they use, how they disseminate their propaganda and how they maintain an online presence despite counter-measures against it.[46]

These two categories also correspond with two different categories in the literature on counter-terrorism online. One type of literature focuses on how to respond and counter the propaganda from the Islamic State, through, for instance, counter-narratives.[47] Another category focuses more on the technical and judicial aspects of preventing the Islamic State and similar groups from using the Internet for propaganda and recruitment purposes.[48]

This is not a new development – the Internet has been central for the propaganda and recruitment strategy of most terrorist groups for a number of years. However, as with the their use of drones, the rise of the Islamic State coincided with a rapid technological advance in the form of the development and popularisation of a vast array of apps and platforms the Islamic State could exploit.[49] Especially important was the popularisation of apps that provided end-to-end encryption, such as Telegram and WhatsApp .[50] The proliferation of encrypted apps has made it easier and safer for members and sympathisers of the Islamic State to communicate with each other and to meet potential recruits online. Especially worrying is the new phenomenon of so-called remote-controlled plots and virtual entrepreneurs grooming and micro-managing potential attackers through various encrypted social media platforms.[51] Encrypted apps have been reportedly used immediately before or during attacks in Europe where handlers abroad communicate with a remotely-controlled operative.[52]

The online community of sympathisers has also contributed to the technological advances of the Islamic State (and similar groups) through posting instruction manuals and how-to-tips online, for instance, on how to increase the range of drones or how to communicate securely.[53] In February 2016 a Telegram channel for "Islamic State Scientists & Engineers" was launched. The channel was only open to those who had pledged allegiance to the Caliph and who had a technical degree such as engineering, aeronautics, physics and biology. The stated intent behind the channel was to gather a group of qualified people who could do research in order to support "the military industry in the Islamic State."[54]

The Islamic State was of course far from the only terrorist group capable to take advantage of the opportunities provided by new communications technology. Yet, as with the Islamic State's attacks with chemical weapons, the group distinguishes itself mainly through the scale and volume of its use of Internet and social media. The extent of IS' territorial control and the sheer number of attacks committed by the group, provided it with a large reservoir of battle footage and pictures that could be turned into slick productions that gained worldwide distribution. Like its predecessor al-Qaida in Iraq, the Islamic State has exploited the new technology to receive worldwide attention by broadcasting brutal executions. Abu Musab al-Zarqawi, regarded by the Islamic State as its historical founder, gained worldwide notoriety in 2004 when he was seen beheading the U.S hostage Nicholas Berg in the first video issued by his group on the Internet. This was years before the rise of social media; the video was released on the jihadi web forum that was the main platform for disseminating jihadi material at the time. The movie did, however, gain attention far beyond the jihadi forums - the search string "Nick Berg" was the second most popular Google search for May 2004, second only to "American Idol".[55]

Islamic State has not only used the Internet to distribute propaganda, but also for more offensive purposes, mainly through its so-called "Cyber Caliphate Army" (*jaysh al-khilafa al-iliktruni*).[56] However, this "Army" has primarily been engaged in what has been referred to as cyber vandalism and hacktivism. So far the general assessment is that the Islamic State capabilities in the realm of cyber are low and unsophisticated.[57] It has also been claimed that some of the activities of the Cyber Caliphate originated from Russia.[58] Moreover, there have been reports that Islamic State members and/or supporters have used virtual currencies such as Bitcoin, but so far the evidence is mainly anecdotal.[59] The Islamic State has also been accused of using the Internet for raising money, for instance, through fake eBay transactions.[60]

To sum up, the most innovative use of the Internet by the Islamic State is that they have been using encryption not only in order to spread propaganda but also for offensive purposes by remotely directing and coaching operatives immediately before and during ongoing terrorist operations.

Innovation in Zones of Ongoing Armed Conflict

Although both capabilities and intention are crucial factors for estimating the potential technological threat from a non-state actor, the perhaps most important factor is the question of *priority.* For instance, if the Islamic State and its predecessor have been experimenting to develop and use chemical weapons since 1999, with few enemy casualties, it can hardly be said to have been a "success" from the viewpoint of the terrorists - the more so when compared to the staggering number of casualties these groups have been responsible for through other and less technological advanced modi operandi.

Thus, given that there exists technologically less advanced and less resource-intensive modi operandi that have proven to be more effective in terms of creating deaths and destruction, the question raises: why and under what circumstances would a non-state actor decide to allocate a large amount of its (usually limited) resources to develop more advanced technology? This question is not properly addressed in the literature, but a promising avenue of research that might help to answer such a question is by studying the internal decision-making processes and the internal organisation of terrorist groups. For instance, how do terrorist groups manage their resources? How does a group that frequently loses resourceful professionals and key leaders secure organisational learning and transfer knowledge within the organisation? How are terrorist groups set up for processes such as innovation, adaption and training?[61] It has been pointed out that due to the lack of sources that there has been a paucity of studies on the internal decision-making of terrorist groups or the background of its recruits.[62] However, due to the increasing availability of internal documents and lists of members from the Islamic State, it is now possible to gain a better insight into the internal processes of IS.[63]

It is beyond the scope of this article to provide in-depth analysis of these questions. This review has, however, illustrated that one favorable condition for non-state actors acquiring and using more advanced technology is territorial control. For instance, all of the insurgent groups with discernable drone programs had territorial control and three out of four were involved in the conflict in Syria. Previous studies of terrorist innovation have also found that territorial control and operating in an armed conflict zone offering frequent possibilities to test innovations often are drivers for technological progress.[64]

In Iraq and Syria, the Islamic State's territorial control has also enabled the group to experiment with less advanced technology in a DIY-way. According to internal documents, the Islamic State had a separate Research and Development Division (*Qism al-buhuth w al-tatwir*). This division experimented, for instance, with producing remote-control car bombs, a robot operated by a solar-panel that was intended to function as a decoy, an automatic steering system for artillery weapons, etc.[65] Sky News was provided with several hours of unedited videos by a Syrian rebel group, showing documentation of what is referred to as an Islamic State "jihad university" in Raqqa. The video shows how the Islamic State is experimenting with developing a driverless car bomb.[66] The Islamic State has also constructed a fleet of armored cars, with a high DIY improvised "Mad Max" factor.[67] Insurgent groups operating in Syria have also been experimenting with various forms of remotely-controlled and tele-operated weapons.[68]

Conclusion: "Low-Tech Terrorism"?

This review of the Islamic State's use of technology has found that what distinguishes the group's use of technology from other non-state actors is primarily its ability to exploit the opportunities offered by commercial technology development as well as the extent of its use of technology. This is primarily an effect of the unprecedented size of the Islamic State. Another explanation is that the rise of the Islamic State partly coincided with a rapid technological development within the fields of drone and communication technology. In that sense, the Islamic State was uniquely poised to exploit this, given its size and the degree of its territorial control.

Another observation is that terrorist groups, including the Islamic State, mainly use technology for defensive and not offensive operations. As an illustration, a large share of the technological innovation and concern from Islamic State and al-Qaida has been within the field of operational security and how to defend and protect the organisation from the technology used against them. For instance, until recently most of the publications from al-Qaida were concerned with how to protect themselves from U.S. drones rather than focusing on how to use drones themselves.[69] The Islamic State and its supporters online have also spent considerable resources and energy on how to maintain their presence on Twitter and other social media platforms and how to communicate securely, sharing information on digital security and encryption.[70]

This review has illustrated that even in cases when the Islamic State used more advanced technology, such as drones, or attempted to use CBRN weapons, the group has done so in an improvised, crude and DIY manner. Even a terrorist group like the Islamic State, with its unprecedented access to resources, is incomparable in strength to a real state. The group's primary asset is its innovative use of already existing technologies and modi operandi, like booby-trapped drones. This is also supported by previous research that has found that the primary originality and innovation of terrorists has historically been to creatively modify or combine pre-existing and relatively "simple" modi operandi.[71]

This underlines the difficulties for a non-state actor to acquire and use more advanced technology. However, it may also indicate that to acquire advanced technology is not a priority for most terrorist groups. The primary knowledge gap identified by this literature review is precisely the question of prioritisation – why and under what circumstances would a terrorist group decide to use some of its limited resources in order to acquire new technological capabilities? In order to answer this question, it is necessary to gain a more in-depth insight into internal factors such as various groups' internal decision-making and what role technology and innovation plays in the strategic thinking of the groups' leaders.

Finally, what are the implications for use of technology in terrorist attacks in areas outside the conflict theater, e.g. in Europe? While there has been some technological innovation in conflict areas like Iraq and Syria, recent studies of the modus operandi of jihadi terrorism in Europe indicate that terrorists have become *less* technologically advanced – using relatively "low-tech" means such as knives, firearms and rented vehicles as weapons.[72] This is also something that has been recommended both by the Islamic State and by al-Qaida in their respective online publications.[73] Al-Qaida in the Arabian Peninsula (AQAP) hailed the perpetrator who on 22 March 2017 drove a car into pedestrians on London's Westminster Bridge for employing "the art of the possible" and urged other lone wolves to do the same.[74]

This has led some observers to refer to a trend of "low-tech terrorism" where terrorists "routinely transform everyday tools into low-tech weapons or attack vehicles—whether cars, trucks, scooters, or kitchen knives".[75] This is probably an adaption to the growth of security measures in Europe, but it also illustrates and supports previous studies concluding that terrorists tend to be pragmatic and conservative in terms of their uses of technology and their modus operandi.[76]

In terms of technological innovation, this implies that terrorist groups in the West will primarily use relatively simple, but easily accessible, commercially available technology that could potentially be transformed into a weapon. For instance, one potential scenario is to steer a swarm of drones towards a crowd, using the drone blades themselves to inflict damage on the crowd or to use drones as part of a coordinated attack.[77] In 2017 it was reported that the Islamic State had achieved a swarm-level capacity of drone use. [78] We have also seen that various encrypted apps have enabled handlers based in a conflict area to remotely assist and guide attackers in Europe – something that is likely to continue.

In the immediate future, there are also other technological developments that can be exploited by the Islamic State or other terrorist organizations, like 3D printing. This allows terrorists to produce parts to a drone for instance, or even 3D printed firearms.[79] There have so far not been any incidents of 3D printed firearms among terrorists registered, but there have been instances of 3D printing used by criminals and drug-cartels.[80] In the longer term, the rapid technological development and increasing commercialisation of new technologies may lead to terrorism taking unexpected turns.

***About the Author:* Truls Hallberg Tønnessen** *is a Research Fellow at the Norwegian Defence Research Establishment (FFI), specialising in Salafi-jihadi insurgent groups in Iraq and Syria. In 2016, he was a visiting scholar at the Center for Security Studies, Georgetown University. He obtained his PhD in history from the*

University of Oslo in 2015, with a dissertation on the rise of al-Qaida in Iraq in 2003-2006. Follow @trulstonnessen

Notes

[1] Wolfgang Rudischhauser, "Could ISIL Go Nuclear?," *NATO Review*, 2015 and Nomi Bar-Yaacov, "What If Isis Launches a Chemical Attack in Europe?," *The Guardian*, 27 November 2015.

[2] For a recent overview of the literature see Brecht Volders and Tom Sauer, eds., *Nuclear Terrorism: Countering the Threat*, (London: Routledge, 2016).

[3] Nicole Alexandra Tishler, "C, B, R, or N: The Influence of Related Industry on Terrorists' Choice in Unconventional Weapons," *Canadian Graduate Journal of Sociology and Criminology* 2 (2), 2013: 52–72, Nada Eweiss, "Non-State Actors & WMD: Does ISIS Have a Pathway to a Nuclear Weapon?" *British American Security Information Council*, March 2016 and Dina Esfandiary and Matthew Cottee, "The Very Small Islamic State WMD Threat," *Bulletin of the Atomic Scientists*, 15 October 2014.

[4] See for instance Peter D. Zimmerman, "Do We Really Need to Worry? Some Reflections on the Threat of Nuclear Terrorism," *Defence Against Terrorism Review* 2 (2), 2009: 1–14; Reshmi Kazi, "The Correlation between Non-State Actors and Weapons of Mass Destruction," *Connections* 10 (4) 2011: 1–11.

[5] For a critical view see for instance Keir A. Lieber and Daryl G. Press, "Why States Won't Give Nuclear Weapons to Terrorists," *International Security* 38 (1) 2013: 80–104.

[6] Stephanie E. Meulenbelt and Maarten S. Nieuwenhuizen, "Non-State Actors' Pursuit of CBRN Weapons: From Motivation to Potential Humanitarian Consequences," *International Review of the Red Cross* 97 (899) July 2016: 831–58, Beyza Unal and Susan Aghlani, "Use of Chemical, Biological, Radiological and Nuclear Weapons by Non-State Actors: Emerging Trends and Risk Factors" *Chatham House - the Royal Institute of International Affairs*, 2016.

[7] Rolf Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?* (Cambridge, MA.:Belfer Center for Science and International Affairs, January 2010), and Meulenbelt and Nieuwenhuizen, "Non-State Actors' Pursuit of CBRN Weapons," *International Review of the Red Cross* 97 (899) July 2016: 831–58.

[8] In 2014 then British Home Secretary Theresa May warned that ISIL, if given support from states, could acquire "chemical, biological or even nuclear weapons to attack us". "Theresa May: Speech to Conservative Party Conference 2014," accessible from http://press.conservatives.com/post/98799073410/theresa-may-speech-to-conservative-party For more examples see Esfandiary and Cottee, "The Very Small Islamic State WMD Threat."

[9] Gary A. Ackerman, "Jihadists and WMD: A Re-Evaluation of the Future Threat," *CBRNe World*, October 2014.

[10] Petter Nesser and Anne Stenersen, "The Modus Operandi of Jihadi Terrorists in Europe," *Perspectives on*

Terrorism 8 (6) 2014: p. 7.

[11] Anne Stenersen, "Toxic Taster: Jihadists' Chemical Weapons Use Remains Crude," *Jane's Intelligence Review* (April 2015), 44-49.

[12] University of Maryland, «Global Terrorism Database»; URL: https://www.start.umd.edu/gtd/ .

[13] Chris Quillen, "The Islamic State's Evolving Chemical Arsenal," *Studies in Conflict & Terrorism* 39 (11) April 2016: 1019–30 and Peter Bergen, "Al Qaeda's Track Record with Chemical Weapons," *CNN*, 7 May 2013.

[14] For a detailed overview of the group's experimenting with chemical weapons see Quillen, "The Islamic State's Evolving Chemical Arsenal."

[15] Bruce Hoffman, "Low-Tech Terrorism," *National Interest*, March - April 2014.

[16] Columb Strack, "Islamic State's chemical weapons capability degraded," *IHS Markit*, 29 June 2017.

[17] Helene Cooper and Eric Schmitt, "ISIS Detainee's Information Led to 2 U.S. Airstrikes, Officials Say," *The New York Times*, 9 March 2016 and Andrea Taylor, "FACTBOX: Evolution of the Islamic State's Chemical Weapons Capacity," *Atlantic Council*, 23 November 2015.

[18] Beatrix Immenkamp, "ISIL/Da'esh and 'Non-Conventional' Weapons of Terror," *European Parliamentary Research Service*, December 2015, Quillen, "The Islamic State's Evolving Chemical Arsenal," and C.J Chivers, "ISIS Has Fired Chemical Mortar Shells, Evidence Indicates," *The New York Times*, 17 July 2015.

[19] Geoffrey Chapman, "Islamic State and Al-Nusra: Exploring Determinants of Chemical Weapons Usage Patterns," *Perspectives on Terrorism*, Vol. XI, Issue 6, December 2017.

[20] See for instance Higgins, “A History of Sarin Use in the Syrian Conflict,” *Bellingcat*, 6 September 2017 and

“Death by Chemicals: The Syrian Government’s Widespread and Systematic Use of Chemical Weapons,” *Human Rights Watch*, 1 May 2017.

[21] Rudischhauser, “Could ISIL Go Nuclear?”, Joby Warrick and Loveday Morris, “How ISIS Nearly Stumbled on the Ingredients for a ‘dirty Bomb,’” *Washington Post*, 22 July 2017.

[22] Rob Downes and Geoffrey Chapman, “Dirty Business - Challenges remain to Islamic State RDD usage,” *IHS Jane’s Intelligence Review,* April 2016.

[23] Stephen Hummel, “The Islamic State and WMD: Assessing the Future Threat,” *CTC Sentinel* 9 (13) 2016: 18–21.

[24] “The Perfect Storm,” *Dabiq,* Issue 9, May 2015, pp.74 - 77.

[25] Lieber and Press, “Why States Won’t Give Nuclear Weapons to Terrorists.” See also Carole N. House, “The Chemical, Biological, Radiological, and Nuclear Terrorism Threat from the Islamic State,” *Military Review* 96 (5) 2016: 68 and Esfandiary and Cottee, “The Very Small Islamic State WMD Threat.”

[26] Ian Johnston, “Brussels attacks: Belgium fears Isis seeking to make ‘dirty’ nuclear bomb,” *The Independent*, 25 March 2016, Gregory S. Jones, “ISIS and Dirty Bombs,” *RAND*, 3 June 2016 and Pamela S. Falk, “The Dirty Bomb Threat,” *Foreign Affairs*, 4 April 2017.

[27] Siobhan McFadyen, “ISIS Plotting Biological Warfare: Brussels Jihadi Found with Bag of Animal Testicles,” *The Express*, 6 May 2016.

[28] Patrick Malone and Jeffrey R. Smith, “The Islamic State’s Plot to Build a Radioactive ‘Dirty Bomb,’” *Foreign Policy* 29 February 2016. For more on topic of insider threat see Matthew Bunn and Scott D.Sagan, *Insider Threats* (Cornell University Press, 2017).

[29] The most detailed reports on Islamic State and drones are Don Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology,” *Combating Terrorism Center*, October 2016, Don Rassler, Muhammad al-Ubaydi, and Vera Mironova, “CTC Perspectives – The Islamic State’s Drone Documents: Management, Acquisitions, and DIY Tradecraft” *Combating Terrorism Center*, 31 January 2017, Nick Waters, “Types of Islamic State Drone Bombs and Where to Find Them,” *Bellingcat*, 24 May 2017 and Asaad Almohammad and Anne Speckhard, “ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics” *The International Center for the Study of Violent Extremism*, 5 May 2017.

[30] Don Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology,” *Combating Terrorism Center*, October 2016.

[31] Ibid.

[32] Asaad Almohammad and Anne Speckhard, “ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics” *The International Center for the Study of Violent Extremism*, 5 May 2017.

[33] “Islamic State’s Weaponised Drones,” *Conflict Armament Research*, 2016 and Joby Warrick, “Use of Weaponized Drones by ISIS Spurs Terrorism Fears,” *Washington Post*, 21 February 2017.

[34] Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology.”

[35] Ibid.

[36] Bayt al-Maṣādir, “[Image] Islamic State – Al-Yaqīn Foundation: ‘Drones of the Islamic State – Until: 1st March 2017 – One Month,’” *Bayt Al-Maṣādir*, 1 March 2017.

[37] Eric Schmitt, “Pentagon Tests Lasers and Nets to Combat a Vexing Foe: ISIS Drones,” *New York Times*, 23 September 2017.

[38] Don Rassler, Muhammad al-Ubaydi, and Vera Mironova, “CTC Perspectives – The Islamic State’s Drone Documents: Management, Acquisitions, and DIY Tradecraft,” *Combating Terrorism Center*, 31 January 2017.

[39] Asaad Almohammad and Anne Speckhard, “ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics” *The International Center for the Study of Violent Extremism*, 5 May 2017.

[40] Linda Robinson, “Assessment of the Politico-Military Campaign to Counter ISIL and Options for Adaptation,” RAND, 2016.

[41] Catherine Shu, “DJI Adds Much of Iraq and Syria to Its List of No-Fly Zones for Its Drones,” *TechCrunch*, 27 April 2017 and Gareth Corfield, “Drone Maker DJI Quietly Made Large Chunks of Iraq, Syria No-Fly Zones,” *The Register*, 26 April 2017.

[42] Thomas Gibbons-Neff, “The U.S. Is Apparently Using Anti-Drone Rifles against the Islamic State,” *Washington Post*, 26 July 2016.

[43] Brynjar Lia, *Globalisation and the Future of Terrorism: Patterns and Predictions* (London: Routledge, 2005), 170–71.

[44] Adam Hoffman and Yoram Schweitzer, "Cyber Jihad in the Service of the Islamic State (ISIS)," *Strategic Assessment* 18 (1) 2015: 71–81, "Overview of Daesh's Online Recruitment Propaganda Magazine, Dabiq" *The Carter Center*, December 2015). P.W Singer and Emerson Brooking, "Terror On Twitter: How ISIS Is Taking War To Social Media," *Popular Science*, 11 December 2015 and Walid Magdy, Kareem Darwish, and Ingmar Weber, "#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support," *First Monday* 21 (2) 2016.

[45] Charlie Winter, "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy," *Quilliam Foundation*, July 2015, Haroro J. Ingram, "An Analysis of Islamic State's Dabiq Magazine," *Australian Journal of Political Science* 51 (3) 2016: 458–77, Brandon Colas, "What Does Dabiq Do? ISIS Hermeneutics and Organizational Fractures within Dabiq Magazine," *Studies in Conflict and Terrorism* 40 (3) 2016: 173–90, Monica Maggioni and Paolo Magri, "Twitter and Jihad: The Communication Strategy of ISIS" *Italian Institute for International Political Studies*, 2015) and Harleen Gambhir, "The Virtual Caliphate: ISIS's Information Warfare" *Institute for the Study of War*, December 2016).

[46] Ali Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence," *Perspectives on Terrorism* 9 (3) 2015: 3–20. J.M Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *Brookings Institution*, March 2015). N. F. Johnson et al., "New Online Ecology of Adversarial Aggregates: ISIS and beyond," *Science* 352 (6292) 2016: 1459–63, Ali Fisher and Nico Prucha, "The Call-up: The Roots of a Resilient and Persistent Jihadist Presence on Twitter," *Combating Terrorism Exchange* 4 (3) 2014), J.M Berger and Heather Perez, "The Islamic State's Diminishing Returns on Twitter" *The Program on Extremism, George Washington University*, February 2016.

[47] Alberto M Fernandez, "Here to Stay and Growing: Combating ISIS Propaganda Networks" *Brookings Institution*, 2015, Jared Cohen, "How To Fight The Islamic State Online," *Foreign Affairs* 94 (December 2015).

[48] Elizabeth Bodine-Baron et al.,"Examining ISIS Support and Opposition Networks on Twitter" *RAND* 2016 and Berger and Perez, "The Islamic State's Diminishing Returns on Twitter."

[49] For an overview of various platforms and apps see Laith Alkhouri and Alex Kassirer, "Tech for Jihad: Dissecting Jihadists' Digital Toolbox Archives," *Flashpoint,* July 2016.

[50] Ahmad Shehabat, Teodor Mitew, and Yahia Alzoubi, "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West," *Journal of Strategic Security* 10 (3) 2017: 27–53 and Jamie Bartlett and Alex Krasodomski-Jones, "Online Anonymity - Islamic State and Surveillance," *Demos*, March 2015

[51] See for instance Alexander Meleagrau-Hitchens and Seamus Hughes, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," *CTC Sentinel* 10 (3) 2017: 1–8. Daveed Gartenstein-Ross and Madeleine Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation," *War on the Rocks*, 4 January 2017.

[52] See for instance Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar," *The New York Times*, 4 February 2017.

[53] Nico Prucha, "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram," *Perspectives on Terrorism* 10 (6) 2016: 48–58 and Steven Stalinsky and R. Sosnow "A Decade Of Jihadi Organizations' Use Of Drones – From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones," *MEMRI*, 21 February 2017. See also Anne Stenersen, "'Bomb-Making for Beginners': Inside Al Al-Qaeda E-Learning Course," *Perspectives on Terrorism* 7 (1) 2013: 25–37

[54] Stalinsky and Sosnow, "Jihadi Drones - ISIS Al-Qaeda Hamas Hizbullah & Others."

[55] Gabriel, Weimann, *Terror on the Internet.* (Washington D.C: United States Institute of Peace Press, 2006), p. 110.

[56] Hoffman and Schweitzer, "Cyber Jihad in the Service of the Islamic State (ISIS)," 73–74.

[57] Laith Alkhouri, Alex Kassirer, and Allison Nixon, "Hacking For ISIS: The Emergent Cyber Threat Landscape," *Flashpoint*, April 2016), Jose Pagliery, "ISIS Is Attacking the U.S. Energy Grid (and Failing)," *CNN*, 16 October 2015, Jack Moore, "ISIS Cyber Jihadis Are 'garbage' at Hacking, Top Researcher Says," *Newsweek*, 26 September 2017.

[58] "Islamischer Staat'-Cyberattacken Als Werk Russischer Hacker Enttarnt," *Spiegel Online*, 18 June 2016

[59] Zachary K. Goldman et al., "Terrorist Use of Virtual Currencies" (Washington D.C: Center for a New American Security, May 3, 2017), Iwa Salami, "Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat This?," *Studies in Conflict and Terrorism*, August 11, 2017.

[60] McCallister, "ISIS Used eBay As Part of Terror Network, Unsealed FBI Affidavit Shows," *NPR*, 11 August 2017.

[61] Truls Hallberg Tønnessen, "Training on a Battlefield: Iraq as a Training Ground for Global Jihadis," *Terrorism and Political*

Violence 20 (4) 2008: 543–62, Mia Bloom, "Constructing Expertise: Terrorist Recruitment and 'Talent Spotting' in the PIRA, Al Qaeda, and ISIS," *Studies in Conflict and Terrorism* 40 (7) 2017: 603–23 and Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics and Global Trends*, (London: Routledge, 2007).

[62] Rassler, "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology." Meulenbelt and Nieuwenhuizen, "Non-State Actors' Pursuit of CBRN Weapons." Rudischhauser, "Could ISIL Go Nuclear?"

[63] Aymenn Jawad Al-Tamimi, "Archive of Islamic State Administrative Documents," accessible from http://www.aymennjawad.org/2016/01/archive-of-islamic-state-administrative-documents-1, 11 January 2016 and Johnston et al. Foundations of the Islamic State: Management, Money, and Terror in Iraq, 2005–2010. (Santa Monica: RAND Corporation, 2016)

[64] Dolnik, Understanding Terrorist Innovation, p.152.

[65] "New ISIS Document Reveals Group's Electronic Warfare Projects," *Zaman al-was*l, 19 February 2017.

[66] Stuart Ramsay "Exclusive: Inside IS Terror Weapons Lab," *Sky News,* 5 January 2016.

[67] Jamie Seidel, "Islamic State Goes 'Mad Max' in Its Fight for Mosul with Homemade Armoured Vehicles," *News Corp Australia Network*, 31 October 2016.

[68] "Captured Daesh Remote Controlled SVD," *The Firearm Blog*, 3 June 2015. For an overview of how various insurgent groups have employed remote controlled arms in Syria see Robert J. Bunker and Alma Keshavarz, "Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns" (Foreign Military Studies Office, 2016).

[69] Stalinsky and Sosnow, "Jihadi Drones - ISIS Al-Qaeda Hamas Hizbullah & Others," 43–46 and Don Rassler, "Drone, Counter Drone: Observations on the Contest Between the United States and Jihadis," *CTC Sentinel* 10 (1) 2017: 23–27.

[70] Edward Blake, "Islamic State Supporters Share Edward Snowden Video to Explain Need for Encryption," *Washington Times*, 11 February 2016. For an overview see Berger and Perez, "The Islamic State's Diminishing Returns on Twitter."

[71] Lia, *Globalisation and the Future of Terrorism: Patterns and Predictions*. Hoffman, "Low-Tech Terrorism."

[72] See for instance Petter Nesser and Anne Stenersen, 'The Modus Operandi of Jihadi Terrorists in Europe', *Perspectives on Terrorism* 8, no. 6 (18 December 2014) and Petter Nesser, Anne Stenersen, and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect," *Perspectives on Terrorism* 10, no. 6 (2016): 3

[73] See for instance Alastair Reed and Haroro Ingram, "Exploring the Role of Instructional Material in AQAP's Inspire and ISIS' Rumiyah" (The Hague: ICCT, 2016).

[74] "Inspire Guide, Issue 5: The British Parliament Operation in London," *al-Malahim Media*, 23 March 2017. URL: https://azelin.files.wordpress.com/2017/04/al-qacc84_idah-in-the-arabian-peninsula-e2809cinspire-guide-5-the-british-parliament-operation-in-london22.pdf .

[75] Corri Zoli, "Lone-Wolf or Low-Tech Terrorism? Emergent Patterns of Global Terrorism in Recent French and European Attacks," *Lawfare*, 17 August 2016 and Bruce Hoffman, "Low-Tech Terrorism," *The National Interest*, April 2014.

[76] B. Lia, *Globalisation and the Future of Terrorism: Patterns and Predictions*. Hoffman, "Low-Tech Terrorism."

[77] "Hostile Drones: The Hostile Use of Drones by Non-State Actors against British Targets," *Oxford Research Group*, January 2016 and Stalinsky and Sosnow, "Jihadi Drones - ISIS Al-Qaeda Hamas Hizbullah & Others."

[78] Christopher Dickey,"As ISIS Prepares Its Terror Resurrection, Watch Out for Drone 'Swarms,'" *The Daily Beast*, 28 February 2017.

[79] Larry Friese, "Special Report No. 2: Emerging Unmanned Threats – The Use of Commercially-Available UAVS by Armed Non-State Actors," *Armament Research Services*, 8 February 2016.

[80] Robert J. Bunker, "Home Made, Printed, and Remote Controlled Firearms," *Trends Institution*, 21 June 2015.