



**Universiteit  
Leiden**  
The Netherlands

## **Learning from foes: how racially and ethnically motivated violent extremists embrace and mimic Islamic state's use of emerging technologies**

Veilleux-Lepage, Y.D.; Daymon, C.; Archambault, E.

### **Citation**

Veilleux-Lepage, Y. D., Daymon, C., & Archambault, E. (2022). *Learning from foes: how racially and ethnically motivated violent extremists embrace and mimic Islamic state's use of emerging technologies*. London: Global Network on Extremism & Technology. Retrieved from <https://hdl.handle.net/1887/3485437>

Version: Publisher's Version

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/3485437>

**Note:** To cite this publication please use the final published version (if applicable).



Global Network  
on Extremism & Technology

# Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies

---

Yannick Veilleux-Lepage, Chelsea Daymon and Emil Archambault

*GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.*

*The authors of this report are  
Yannick Veilleux-Lepage, Chelsea Daymon  
and Emil Archambault*

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

## **CONTACT DETAILS**

For questions, queries and additional copies of this report, please contact:

ICSR  
King's College London  
Strand  
London WC2R 2LS  
United Kingdom

T. **+44 20 7848 2098**

E. **[mail@gnet-research.org](mailto:mail@gnet-research.org)**

Twitter: **[@GNET\\_research](https://twitter.com/GNET_research)**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at [www.gnet-research.org](http://www.gnet-research.org).

© GNET

# Executive Summary

While the existence of terrorist alliances is well documented in terrorism studies,<sup>1</sup> how terrorist groups learn from and mimic their adversaries' tactics, techniques and procedures (TTPs) remains largely unexplored. Building on existing terrorist innovation literature, this report introduces a framework to understand what factors can propel or hinder a terrorist group's adoption of new TTPs.

Focusing on three emerging technologies – namely, cloud-based messaging applications, weaponised unmanned aerial vehicles and social media bots – this report traces how racially and ethnically motivated violent extremists (REMVE) adopted or failed to adopt practices originating with Islamic State. This report explains this (non-)adoption through three sets of factors: technical, group and knowledge transfer. It argues that technical ease, similarities in group structure and online communication environments, and available knowledge-transfer channels explain why REMVE adopted Islamic State's practice of employing cloud-based messaging applications such as Telegram. Conversely, inverse dynamics – high technical costs and lower-cost alternatives, different group structures, goals, constituencies and a lack of descriptive knowledge transfer – explain why REMVE use of drones has remained marginal. Finally, despite REMVE's adoption of cloud-based messaging applications, their differing communication objectives and a more permissive online environment led them to rely far less on bot technology than Islamic State did.

---

<sup>1</sup> See Victor H. Asal, Hyun Hee Park, R. Karl Rethemeyer and Gary Ackerman, "With Friends Like These... Why Terrorist Organizations Ally," *International Public Management Journal* 19, no. 1 (2016): pp. 1–30; Tricia Bacon, "Alliance Hubs: Focal Points in the International Terrorist Landscape," *Perspectives on Terrorism* 8, no. 4 (2014): pp. 4–26; Tricia Bacon, *Why Terrorist Groups Form International Alliances* (Philadelphia: University of Pennsylvania Press, 2018); Navin A. Bapat and Kanisha D. Bond, "Alliances Between Militant Groups," *British Journal of Political Science* 42, no. 4 (2012): pp. 793–824; and Michael C. Horowitz and Philip B. K. Potter, "Allying to Kill: Terrorist Intergroup Cooperation and the Consequences for Lethality," *Journal of Conflict Resolution* 58, no. 2 (2014): pp. 199–225.





# Overview

This report concerns itself with terrorist technical innovation, particularly with regards to terrorists' incorporation of emerging technologies into their practices. More specifically, it investigates, through the elaboration of a theoretical learning framework, how terrorist groups can adopt the practices of ideological enemies operating in different security, ideological and political environments. It does so through a study of three cases of emerging technology use by Islamic State (IS) and racially and ethnically motivated violent extremists (REMVE), which shed light on why ideologically diverse groups might adopt practices from each other.

The theoretical framework described in this study highlights numerous elements that can help or hinder a terrorist group's adoption of new techniques, tactics or procedures (TTPs). Technical characteristics, group factors and knowledge-transfer factors are the three main kinds of elements that determine how extremist groups learn. These three types of characteristics help to explain why groups do or do not adopt practices associated with ideological adversaries. In addition to learning from patrons and allies and inventing new techniques, terrorist groups sometimes adopt practices associated with ideological foes; this report analyses such cases with particular regard to the transmission (and non-transmission) of TTPs from IS to REMVE.

This report considers three emerging technologies and how their use (or non-use) by REMVE was influenced by prior practices by IS. First, the use of cloud-based messaging applications demonstrates direct adoption by REMVE of IS practices. Similar environmental restrictions, group dynamics and the presence of explicit knowledge transfer explain such adoption. Second, whereas IS established an advanced drone programme, the use of drones by REMVE remains marginal and largely distinct from IS practices. REMVE found themselves in different environments, pursuing different objectives with varying resource levels; they preferred "tried and tested" techniques (such as mass shootings), which were less complex, less resource-intensive and more compatible with prevailing techniques. Finally, whereas IS relied heavily on bot technology to thrive in a hostile online environment, leveraging a group structure constructed around highly centralised media production units and unaffiliated sympathisers, REMVE-organised groups have so far refrained from widespread bot usage, given their different objectives and the more permissive online environment in which they operate.

Therefore, this report draws attention to the very broad environments in which violent groups operate beyond their immediate ideological, political and cultural domains. Thus, the broader innovation environments may shape how given groups develop. How groups distribute knowledge among themselves also contributes to ideologically opposed groups adopting each other's practices;

for instance, IS's decision to publish materials in English, in order to reach its English-speaking base of sympathisers, facilitated knowledge transfer to REMVE. However, the adoption of new TTPs is not automatic. Technical, group and knowledge-transfer factors remain central to explaining the diffusion and adoption of new violent practices.

# Contents

<u>Executive Summary</u>	<u>1</u>
<u>Overview</u>	<u>3</u>
<u>1 Introduction</u>	<u>7</u>
<u>2 Terrorist Innovation and Mimicry</u>	<u>9</u>
<u>3 Case Study 1: Cloud-Based Instant Messaging Services</u>	<u>15</u>
<u>4 Case Study 2: Unmanned Aerial Vehicles</u>	<u>19</u>
<u>5 Case Study 3: Social Media Bots</u>	<u>23</u>
<u>6 Conclusion</u>	<u>27</u>
<u>Policy Section</u>	<u>29</u>





# 1 Introduction

**T**errorist groups, regardless of ideology, operate in inherently hostile environments. In these sorts of environments, they continuously strive to gain a competitive advantage against their adversaries, whether that be a state and its security apparatus or other terrorist groups striving to appeal to the same constituency. To gain this competitive advantage, terrorist groups innovate either by devising new techniques, tactics and procedures (TTPs) or by adopting the TTPs used by other actors, both friendly and hostile, state and non-state. Terrorist groups who fail to innovate will either “be degraded to the point of irrelevance” or fail to attract resources, recruits and supporters.<sup>2</sup>

In addition to its astonishing brutality, Islamic State (IS) is noteworthy for the innovative ways its TTPs leveraged emerging technologies to defeat its adversaries. While IS was far from the only salafi-jihadist group to leverage emerging technologies, its apparently seamless integration of cloud-based instant messaging applications, unmanned aerial vehicles and social media bots within its TTPs appears to have served as a sort of blueprint for other extremist groups, including racially and ethnically motivated violent extremists (REMVE) in the West. While the existence of alliances among terrorist groups is well established in the existing literature and supplemented with rich empirical accounts of collaboration and information exchange between terrorist groups,<sup>3</sup> how terrorists learn from and sometimes adopt their ideological adversaries’ TTPs and leverage these emerging technologies has remained woefully under-examined.<sup>4</sup>

Building on the literature on terrorist innovation, this report introduces a theoretical framework outlining factors that influence how and in which circumstances extremist groups acquire technical and tactical knowledge from ideological adversaries. These factors belong to three categories: technical factors, group factors and knowledge-transfer factors. Building on this theoretical framework, this report then examines how and to what degree REMVE have sought to acquire knowledge about and adopt IS TTPs. To do so, this report focuses on three emerging technologies central to IS TTPs, which have in turn been adopted to various degrees and with mixed success by REMVE:

2 Daveed Gartenstein-Ross, Matt Shear and David Jones, “Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters,” *Valens Global & Organization for the Prevention of Violence* (20 November 2019): p. 7, <https://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/>.

3 Erica Chenoweth, “Democratic Competition and Terrorist Activity,” *The Journal of Politics* 72, no. 1 (January 2010): pp. 16–30; Eli Karmon, *Coalitions between Terrorist Organizations: Revolutionaries, Nationalists, and Islamists* (Leiden; Boston: Martinus Nijhoff, 2005); Victor Asal and R. Karl Rethemeyer, “The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks,” *The Journal of Politics* 70, no. 2 (April 2008): pp. 437–49; Ami Pedahzur and Arie Perliger, “The Changing Nature of Suicide Attacks: A Social Network Perspective,” *Social Forces* 84, no. 4 (2006): pp. 1987–2008.

4 Some notable exceptions include Marc-André Argentino, Shiraz Maher and Charlie Winter, “Violent Extremist Innovation: A Cross-Ideological Analysis,” *International Centre for the Study of Radicalisation*, (2021), <https://icsr.info/wp-content/uploads/2021/12/ICSR-Report-Violent-Extremist-Innovation-A-Cross%E2%80%91Ideological-Analysis.pdf>; Yannick Veilleux-Lepage, *How Terror Evolves: The Emergence and Spread of Terrorist Techniques* (Rowman & Littlefield, 2020); Daniel Köhler and Julia Ebner, “Strategies and Tactics: Communication Strategies of Jihadists and Rightwing Extremists,” in *Hate Speech and Radicalisation Online*, ed. Johannes Baldauf, Julia Ebner and Jakob Guhl (The OCCI Research Report, 2019): pp. 18–26, <https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>.

cloud-based instant messaging applications, unmanned aerial vehicles and social media bots.

Techniques that work well for one group in a given environment may not work for another due to the three types of factors outlined above; other TTPs can easily travel if the technical, group and knowledge-transfer characteristics correspond. The three cases outlined here cover one successful transfer and two cases where TTPs did not transfer from IS to REMVE. In the first case, the switch from open platforms to cloud-based messaging applications demonstrates REMVE adopting IS practices due to similar external environments, group dynamics and available descriptive knowledge-transfer mechanisms. In the second case, on the contrary, the complex and resource-intensive use of unmanned aerial vehicles saw limited adoption by REMVE, despite some learning channels being available. Group structure as well as ideological and technical compatibility issues privileged the continued use of existing techniques of violence (such as mass shootings), with UAVs being integrated only marginally. Finally, whereas IS found itself facing ongoing crackdowns by social media companies and tackling the desire to promote the Caliphate to large numbers of sympathisers online, both of which incentivised the use of bot technology, the relative permissibility of the online environment for REMVE content as well as different messaging needs led to a lesser reliance on bots.

In sum, this report not only contributes to our understanding of how and why terrorist groups embrace emerging technologies, but also how the malevolent use of emerging technologies can spread from one ideologically motivated social movement to another, dramatically changing the security landscape. From a policy standpoint, knowledge transfer from IS to REMVE can be seen as posing several security risks, as it may:

- (a) Enable REMVE to do new things that they could not do before. For example, it may allow for entirely new TTPs or provide more options for carrying out existing operations more effectively;
- (b) Improve REMVE's abilities to function, for instance by increasing the lethality of operations and the probability of their success or by reducing the risks associated with the use of certain TTPs; and
- (c) Allow REMVE to use certain TTPs already within their means but at lesser cost to them in terms of time, personnel, resources or other forms of output.

## 2 Terrorist Innovation and Mimicry

As Barnett, Maher and Winter keenly articulate in their review of the literature on ‘the interplay’ between REMVE and Islamist extremists, changes in a terrorist group’s TTPs involves two interrelated phenomena: (1) terrorist innovation; and (2) terrorist learning.<sup>5</sup> The former relates to the radical or incremental invention of “new techniques or technologies to achieve unchanging objectives”,<sup>6</sup> whereas the latter relates to the process by which terrorist groups assimilate knowledge and know-how from others. Often, such learning will occur within a given ideological movement, from patron states or allied groups,<sup>7</sup> through direct or informal information sharing. However, in some cases, learning may take place across ideological boundaries and between groups with diametrically opposed ideological outlooks.

Organisational theory holds two analytical frameworks relevant to the notion of terrorist learning: (1) diffusion, which emphasises the passive dissemination of certain TTPs from one actor to another; and (2) adoption, which concerns an actor’s conscious decision to assimilate the necessary know-how to employ new TTPs. Diffusion theory assumes groups will embrace new TTPs when and if they discover their existence, as long as there are no impediments to uptake. Similarly, it is assumed that knowledge about given TTPs is transmitted through simple contacts between existing users and potential new users.<sup>8</sup> However, this theoretical approach has significant drawbacks: namely, that it regards terrorist groups as passive consumers of information, disregarding important factors that hinder a group’s willingness to adopt certain TTPs. In fact, terrorism scholarship has convincingly detailed how mere knowledge of other groups’ TTPs is not a sufficient precondition for the spread of TTPs. For example, while technical and tactical knowledge of suicide bombing has been diffused globally, the technique remains conspicuously absent from several protracted and violent conflicts, an absence that Kalyvas and Sánchez-Cuenca have attributed to the ‘constituency costs’ associated with embracing this technique.<sup>9</sup>

To address this passivity problem, a focus on ‘adoption’ instead concentrates on the specific elements that affect the spread of TTPs from one group to another.<sup>10</sup> In their quest to maintain

5 James Barnett, Shiraz Maher and Charlie Winter, “Literature Review: Innovation, Creativity and the Interplay Between Far-right and Islamist Extremism,” *International Centre for the Study of Radicalisation*, (2021), <https://icsr.info/wp-content/uploads/2021/03/ICSR-Report-Literature-Review-Innovation-Creativity-and-the-Interplay-Between-Far%E2%80%91right-and-Islamist-Extremism.pdf>.

6 Mohammed M. Hafez and Maria Jose Moyano Rasmussen, “Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators,” *United States Defense Threat Reduction Agency Advanced Systems and Concepts Office* (October 2010): pp. 2–3, <https://www.hsdl.org/?view&did=9908>.

7 Veilleux-Lepage, *How Terror Evolves*.

8 Robert T. Holden, “The Contagiousness of Aircraft Hijacking,” *American Journal of Sociology* 91, no. 4 (1986): pp. 874–904, <http://www.jstor.org/stable/2779961>.

9 Stathis N. Kalyvas and Ignacio Sánchez-Cuenca, “Killing Without Dying: The Absence of Suicide Missions,” in *Making Sense of Suicide Missions*, ed. Diego Gambetta (Oxford University Press, 2005): pp. 209–32, <https://doi.org/10.1093/acprof:oso/9780199276998.001.0001>.

10 Kim Cragin et al., “Sharing the Dragon’s Teeth: Terrorist Groups and the Exchange of New Technologies,” *RAND Corporation* (15 March 2007), <https://www.rand.org/pubs/monographs/MG485.htm>.

a competitive advantage over their adversaries, terrorist groups must make active decisions on which tactics, techniques or procedures they will employ. In other words, the adoption of new TTPs is seen as a deliberate, active process rather than a passive one.<sup>11</sup>

The decision to adopt new TTPs involves an important paradox for terrorist organisations. On the one hand, terrorist groups must continuously innovate in order to gain or retain a competitive advantage over their adversaries. However, adopting new TTPs is inherently risky, as doing so involves a cost-benefit judgement that might prove to be incorrect. Moreover, groups' efforts to adopt new TTPs might fail for a variety of reasons and thus the group would pay the costs associated with adopting new TTPs without reaping any of the anticipated benefits.<sup>12</sup> For example, following failed attempts and despite the significant expenditure of resources and energy, both the Jewish Defense League and the Provisional Irish Republican Army abandoned aeroplane hijackings as a tactic and banished it from their repertoires of TTPs.<sup>13</sup>

A number of factors have been identified as playing important roles as to whether a group will choose to adopt another's TTPs. These include: (1) the characteristics of the TTPs; (2) the characteristics of the group adopting new TTPs; and (3) the channels through which the transfer of knowledge related to TTPs occurs. These factors are listed in Table 1.

---

11 Everett M. Rogers, *Diffusion of Innovations*, 5th ed (Hoboken, NJ: Wiley, 1983).

12 Cragin, "Sharing the Dragon's Teeth".

13 Edward F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968–1979* (Westport, Conn: Greenwood Press, 1980); Veilleux-Lepage, *How Terror Evolves*.

Table 1: Factors impacting the adoption of TTPs<sup>14</sup>

1. TTP Characteristics	
Factors	Description
1.1. Compatibility	TTPs that appear compatible with the group's familiar TTPs will be easier to adopt. A group must have a sufficient base of knowledge in order to understand and put new TTPs into practice. <sup>15</sup> For example, a terrorist group that only has prior experience with conventional weapons may find it difficult to embrace biological weapons without significant new information input. <sup>16</sup>
1.2. Complexity	The perceived risk of adopting new TTPs is influenced by how simple or complicated they appear. Simple TTPs are more readily transferable due to their ease of communication than complex ones. TTPs that may be utilised as stand-alone units rather than requiring integration into bigger systems are also easier to implement.
1.3. Resources	The more resource-intensive new TTPs are, the higher the stakes in deciding to adopt them. Resources can include financial assets, access to safe havens or territorial strongholds, or members with specialised technical skills. In their assessment of Aum Shinrikyo's 1995 Tokyo subway attack, Rasmussen and Hafez attributed the group's development of VX nerve agent to its considerable wealth – estimated at \$1 billion at the time – and its ability to attract scientists. <sup>17</sup> Along these lines, Jackson argues that financially robust organisations, such as the Provisional Irish Republican Army or Hezbollah, are more likely to innovate. <sup>18</sup> Additionally, Dolnik demonstrated that groups with a safe haven or geographical stronghold are more likely and/or ready to develop, <sup>19</sup> whereas Tucker claims that domestic terrorist organisations face more obstacles to adapt their TTPs, presumably due to a lack of resources. <sup>20</sup> Low-resource TTPs may also allow a group to pursue different TTPs at the same time, or pursue new TTPs alongside their existing activities, avoiding the risks associated with “putting all their eggs in one basket”.

14 Adapted from Cragin, “Sharing the Dragon’s Teeth”.

15 Brian A. Jackson and John C. Baker, *Aptitude for Destruction* (Santa Monica, CA: RAND Corporation, 2005).

16 Cragin, “Sharing the Dragon’s Teeth”.

17 Hafez and Rasmussen, “Terrorist Innovations in Weapons of Mass Effect”.

18 Brian A. Jackson, “Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption,” *Studies in Conflict & Terrorism* 24, no. 3 (1 May 2001): pp. 183–213, <https://doi.org/10.1080/10576100151130270>.

19 Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics and Global Trends* (London: Routledge, 2007).

20 Jonathan B. Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Belfer Center Studies in International Security (Cambridge, MA: MIT Press, 2000).

## 2. Group Characteristics

In the framework on terrorist learning put forward by Cragin et al., the authors consider the characteristics of “source” groups, such as whether the organisation intends to help the receiver organisation, the level of trust between both groups and the existence of direct interpersonal relationships.<sup>21</sup> However, since this report solely focuses on knowledge transfer between foes, the characteristics of the source organisations are deemed largely irrelevant.

Factors	Description
2.1. Internal group decision structure	Adoption decisions can be made collectively or individually, depending on the group structure. A group's internal structure, including the group's leadership, can play an integral role in defining when and how a group will approach innovation. <sup>22</sup> For example, Schweitzer attributed the Popular Front for the Liberation of Palestine's formidable developments in aeroplane hijacking to the malevolent genius of and propensity for innovation by its leader Wadie Haddad. <sup>23</sup>
2.2. External environment	Activities by outside, adversary organisations or individuals can have an impact on a group's decision to adopt TTPs. While the nature of external environmental pressure can vary, changes in the existing security environment appear to be important drivers for innovation and adoption. For example, after the 2003 Iraq War, Johnson describes how Iraqi insurgents reacted to the United States military's introduction of new equipment (such as V-hull armoured personnel carriers) by quickly adapting their TTPs (notably by using shaped-charge IEDs). <sup>24</sup>
2.3. Constituency	A group's relationship with its own constituency can be both an incentive and a barrier to innovation, with groups choosing not to pursue certain TTPs if they believe they might harm their constituents or their constituents' perception of the group. <sup>25</sup> For example, the Provisional Irish Republican Army was compelled to cease using proxy bombs due to public anger from its supporters. <sup>26</sup>
2.4. Ideology	A terrorist group's ideology may impact its predisposition towards innovation. <sup>27</sup> Pondering the importance of ideology, Winter et al. argued that the “contemporary Salafi-jihadist movement encouraged malevolent creativity when considering the application of new technologies on the battlefield.” <sup>28</sup> Conversely, a group's ideology might also hinder the adoption of particular TTPs. For example, Gill and his collaborators detailed how violent dissident Irish republicans came to reject the use of incendiary devices that utilised a condom as a fuse-delay device because group members refused to store caches of condoms, previously proscribed by the Catholic Church, in their homes. <sup>29</sup>

21 Cragin, “Sharing the Dragon's Teeth”.

22 Dolnik, *Understanding Terrorist Innovation*; Paul Gill et al., “Malevolent Creativity in Terrorist Organizations,” *The Journal of Creative Behavior* 47, no. 2 (2013): pp. 125–51; Daveed Gartenstein-Ross and Thomas Joscelyn, *Enemies Near and Far: How Jihadist Groups Strategize, Plot, and Learn* (Columbia University Press, 2022).

23 Yoram Schweitzer, “Innovation in Terrorist Organizations: The Case of PFLP and Its Offshoots,” *Strategic Insights* 10, no. 2 (2011): pp. 17–29.

24 Dominic Johnson, “Darwinian Selection in Asymmetric Warfare: The Natural Advantage of Insurgents and Terrorists,” *Journal of the Washington Academy of Sciences* 95, no. 3 (2009): pp. 89–112, <https://www.jstor.org/stable/24536315>.

25 Mauro Lubrano, “Navigating Terrorist Innovation: A Proposal for a Conceptual Framework on How Terrorists Innovate,” *Terrorism and Political Violence*, (5 April 2021): <https://doi.org/10.1080/09546553.2021.1903440>.

26 A. R. Oppenheimer, *IRA, the Bombs and the Bullets: A History of Deadly Ingenuity* (Dublin; Portland, OR: Irish Academic Press, 2009).

27 Lubrano, “Navigating Terrorist Innovation”.

28 Charlie Winter, Shiraz Maher and Aymenn Jawad al-Tamimi, “Understanding Salafi-Jihadist Attitudes Towards Innovation,” *International Centre for the Study of Radicalisation* (2021): p. 34, <https://icsr.info/wp-content/uploads/2021/01/ICSR-Report-Understanding-Salafi%E2%80%91Jihadist-Attitudes-Towards-Innovation.pdf>.

29 Gill, “Malevolent Creativity in Terrorist Organizations”.



### 3. Knowledge Transfer Channels

The process by which terrorist groups assimilate the necessary know-how to adopt another groups' TTPs is typically said to occur either through (1) relational channels, as a result of direct communication between groups through their interpersonal networks, or (2) non-relational channels, by observing another group's activities without direct communication. Whereas transmission through relational channels typically occurs between groups that share a common ideology or cause, transmission by non-relational channels does not have the same constraints. As this report concentrates on the knowledge transfer between foes, transmission through relational channels can be largely ignored.

Factors	Description
3.1. Vicarious Transfer	One group can get information about another group's TTPs by "watching it from afar". For instance, it appears that the 1994 hijacking of Air France Flight 8969 by the Algerian Groupe Islamique Armé, who intended to crash the aeroplane into the Eiffel Tower, served at least in part as a source of inspiration for the Bojinka plot, which would eventually materialise as the 9/11 attacks. <sup>30</sup>
3.2 Descriptive Transfer	The necessary knowledge to enact new TTPs can be codified and transferred through manuals, recipes and instructions produced by one group and accessed by another. For instance, a number of English-language how-to instructional materials that IS distributes online have been recycled or adapted from al-Qaeda documents, along with other materials from the broader jihadist community. <sup>31</sup> IS supporters have distributed documents, including the four-part magazine series Jihad Recollections, produced by American jihadist Samir Khan, as well as al-Qaeda in the Arabian Peninsula's Inspire magazine, which was edited by Khan until his death, along with material from al-Shabaab's Gaidi M'Taani. <sup>32</sup> As Clifford notes, when it comes to instructional material, this shows that "pragmatism outweighs ideology in deciding which sources are useful". <sup>33</sup> Language barriers, however, may influence how information travels; as an example, IS published technical instructions in English to reach Western, non-Arabic-speaking sympathisers, influencing the global reach of this knowledge base. <sup>34</sup>

<sup>30</sup> Veilleux-Lepage, How Terror Evolves.

<sup>31</sup> Bennett Clifford, "'Trucks, Knives, Bombs, Whatever:' Exploring Pro-Islamic State Instructional Material on Telegram," *CTC Sentinel* 11, no. 5 (2018), pp. 23–9, <https://ctc.usma.edu/trucks-knives-bombs-whatever-exploring-pro-islamic-state-instructional-material-telegram>.

<sup>32</sup> Oren Adaki, "AQAP Publishes Biography of American Jihadist Samir Khan," *Long Wars Journal*, (25 November 2014), [https://www.longwarjournal.org/archives/2014/11/aqap\\_releases\\_biogra\\_1.php](https://www.longwarjournal.org/archives/2014/11/aqap_releases_biogra_1.php); Maura Conway, Jodie Parker and Sean Looney, "Online Jihadi Instructional Content: The Role of Magazines," in Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald and Lella Nouri, eds., *Terrorists' Use of the Internet: Assessment and Response* 136 (Amsterdam: IOS Press, 2017): pp. 182–93.

<sup>33</sup> Clifford, "Trucks, Knives, Bombs, Whatever", p. 23.

<sup>34</sup> Yannick Veilleux-Lepage, "Retweeting the Caliphate: The Role of Soft-Sympathizers in the Islamic State's Media Strategy," *Turkish Journal of Police Studies/Polis Bilimleri Dergisi* 18, no. 1 (2016): pp. 53–69.

Using the nine factors in Table 1, the following section of this report brings these insights to bear as part of an assessment of knowledge transfer from IS to REMVE.<sup>35</sup> To do so, this report focuses on three emerging technologies central to IS's TTPs, which have in turn been adopted to various degrees and with mixed success by REMVE: (1) cloud-based instant messaging services; (2) unmanned aerial vehicles; and (3) the use of social media bot technology.

---

<sup>35</sup> These factors address whether a group may be inclined to pursue innovative TTPs and learn from ideological foes. Whether a group pursuing new TTPs will be successful, however, is only partially explained by these factors; as a result, explaining success in TTP innovation lies beyond the scope of this paper.

### 3 Case Study 1: Cloud-Based Instant Messaging Services

The widespread adoption of cloud-based messaging applications among the wider public in recent years has been accompanied by their increasing use by nefarious actors, who have sought to take advantage of the benefits that cloud-based messaging applications offer. Cloud-based messaging applications are an important tool for communication, with many applications offering cross-platform use, meaning that they function on multiple systems, operating environments and devices, with several including end-to-end encryption (E2EE).

One of the more documented cases of a terrorist group using cloud-based messaging applications is Islamic State's use of the encrypted messaging application Telegram. It is thought that operatives and supporters of IS were using Telegram as early as 2014,<sup>36</sup> with the first recorded cases dated from early 2015. In November 2015, the platform was employed to communicate and spread propaganda in conjunction with the Paris Attacks.<sup>37</sup> However, 2016 marked a "massive shift" in IS's communication TTPs due to a change in the external environment, when Twitter began aggressively shutting down accounts related to the group, thus prompting it to adapt and accelerate its migration to Telegram.<sup>38</sup> This migration offered IS and its supporters a platform that, as Clifford and Powell argue, helped them to dodge terms of service pressures.<sup>39</sup> Furthermore, the ability to create communities of likeminded individuals through the use of Telegram group chats, along with some of the perceived security features that Telegram offers, helped to make Telegram a favoured platform for IS and its supporters.<sup>40</sup> Indeed, this technology benefits nefarious actors by providing platforms where propaganda can be easily disseminated and distributed, and where likeminded individuals can congregate. It can also expand a group's reach while simultaneously allowing the

36 Ahmad Shehabat and Teodor Mitew, "Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics," *Perspectives on Terrorism* 12, no. 1 (2018): pp. 81–99, <https://www.jstor.org/stable/26343748?seq=4>.

37 Natash Lomas, "After Paris Attacks, Telegram Purges ISIS Public Content," *Tech Crunch* (19 November 2015), <https://techcrunch.com/2015/11/19/telegram-purges-isis-public-channels/>; Rebecca Tan, "Terrorists' Love for Telegram," *Vox* (30 June 2017), <https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter>.

38 See Krishnadev Calamur, "Twitter's New ISIS Policy," *The Atlantic* (5 February 2016), <https://www.theatlantic.com/international/archive/2016/02/twitter-isis/460269/>; Nico Prucha, "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram," *Perspectives on Terrorism* 10, no. 6 (2016): p. 51, <https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2016/issue-6/605-is-and-the-jihadist-information-highway---projecting-influence-and-religious-identity-via-telegram-by-nico-prucha.pdf>; and Yannick Veilleux-Lepage, "A Typology of Islamic State's Social Media Distribution Network," in *Media and Mass Atrocity*, ed. Allan Thompson (Toronto: CIGI Press, 2019), pp. 453–82.

39 Bennett Clifford and Helen Powell, "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram," *Program on Extremism* (June 2019), <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf>.

40 See Mia Bloom and Chelsea Daymon, "Assessing the Future Threat: ISIS's Virtual Caliphate," *Orbis* 62, no. 3 (2018): pp. 372–88; Mia Bloom, Hicham Tiflati and John Horgan, "Navigating ISIS's Preferred Platform: Telegram," *Terrorism and Political Violence* 31, no. 6 (2017): pp. 1,242–54; Prucha, "IS and the Jihadist Information Highway," (2016); and Martyn Frampton, Ali Fisher and Nico Prucha, "The New Netwar: Countering Extremism Online," *Policy Exchange* (2017), <https://policyexchange.org.uk/wp-content/uploads/2017/09/The-New-Netwar-1.pdf>.

selection of members or supporters who are truly devoted to a cause. This is especially the case when groups use vetting processes for entry into private chats on cloud-based messaging applications or other security measures.<sup>41</sup>

Interestingly enough, while Telegram is thought by many to be highly secure due to its E2EE and Secret Chat options, it is actually less secure than other leading messaging applications, such as Signal and WhatsApp.<sup>42</sup> Despite this, Telegram remains a core part of IS's TTPs due to its ease of use (low complexity) and its unique capabilities.<sup>43</sup> Thus, the role of Telegram as a central technology within Islamic State's TTPs is less about security and more about what the application can do for the group or rather its compatibility with IS's objectives. This includes how "friendly" an application is – for example, how long a group and its supporters are able to operate on an application without facing large external pressures, such as account shutdowns, suspensions and removals – and what the application offers users, enabling greater communication, outreach and propaganda dissemination. When considering external environmental pressures, in October 2018 and November 2019 Europol implemented two 'Action Days' aimed towards disrupting jihadist networks on Telegram.<sup>44</sup> Although the 2019 campaign demonstrated a "hugely debilitating impact" to IS,<sup>45</sup> the group still remains on Telegram to this day while REMVE networks and content is largely untouched. Some of the features that Telegram provides include the ability to send documents, videos and images (up to 2GB per file as of 2022), the capability to listen to audio files and watch videos on the application, photo editing, timed self-destructing messages in the Secret Chat option, the sharing of live locations, free unlimited storage online, voice calls, supergroups and bot extensions, among other features. Consequently, the large-file sharing and audio/video capabilities that Telegram offers make the spreading of propaganda effective and efficient. Telegram, therefore, offers IS an easily compatible, low complexity solution that requires few new resources from the group. Furthermore, while the change of messaging applications from Twitter to Telegram was prompted by external factors – namely, major social media company crackdowns on extremist content – this switch aligned with IS's group structure, which privileged the decentralised dissemination of centrally produced content, reaching out to broad constituencies of both highly committed militants and loosely aligned unaffiliated sympathisers.<sup>46</sup>

- 
- 41 Vetting to enter pro-IS chats on Telegram was originally witnessed by one of the authors of this report. This same technique is now being used by REMVE on the platform. Additionally, based on interviews with former extremists, security measures such as password protection and codewords are also being applied to specific groups in cloud-based messaging applications: this way, only devoted members have access to them.
- 42 Zak Doffman, "No, Don't Quit WhatsApp to Use Telegram Instead – Here's Why," *Forbes* (21 February 2021), <https://www.forbes.com/sites/zakdoffman/2021/02/13/why-you-should-stop-using-telegram-instead-of-whatsapp-use-signal-or-apple-imessage/?sh=76a959a235ed>.
- 43 See Bennett Clifford, "Migration Moments: Extremist Adoption of Text-Based Instant Messaging Applications," *Global Network on Extremism & Technology* (November 2020), [https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications\\_V2.pdf](https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications_V2.pdf); Clifford and Powell, "Encrypted Extremism," p. 10; and Chelsea Daymon, "Dissertation Notes" (2021/2022).
- 44 See "Referral Action Day with six EU Member States and Telegram," *Europol*, (5 October 2018), <https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-six-eu-member-states-and-telegram>; and "Referral Action Day Against Islamic State Online Terrorist Propaganda," *Europol*, (22 November 2019), <https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda>.
- 45 Amarnath Amarasingam, Shiraz Maher, and Charlie Winter, "How telegram Disruption Impacts Jihadist Platform Migration," *Centre for Research and Evidence on Security Threats* (January 2021): p. 27, <https://crestresearch.ac.uk/resources/how-telegram-disruption-impacts-jihadist-platform-migration/>.
- 46 Yannick Veilleux-Lepage, "Paradigmatic Shifts in Jihadism in Cyberspace: The Emerging Role of Unaffiliated Sympathizers in Islamic State's Social Media Strategy," *Journal of Terrorism Research* 7, no. 1 (5 February 2016): p. 36, <https://doi.org/10.15664/jtr.1183>.

An integral part of Islamic State's outreach strategy is to use public-facing social media applications to connect with supporters who, soon afterwards, are steered to more closed or secure platforms, such as Telegram.<sup>47</sup> This strategy also appears to have been adopted by REMVE to continue their online communications as more public-facing social media platforms crack down on content and accounts.<sup>48</sup> Groups including the Atomwaffen Division and fringe movements like the Not Fucking Around Coalition and the Boogaloo movement have all recently used communication TTPs similar to those employed by IS and more broadly the wider jihadist community for their online communication and distribution of tactical knowledge.<sup>49</sup> In response to tech company crackdowns on REMVE content, similar to Twitter's banning of salafi-jihadist extremist content a few years earlier, REMVE have reacted in a fashion comparable to IS by migrating to Telegram and similar applications.

Furthermore, REMVE have adopted IS's TTPs "implicitly or explicitly" in changing their communication habits to respond to external environmental changes.<sup>50</sup> This awareness of IS's TTP innovation is demonstrated by REMVE's familiarity with content disseminated by IS. For example, the Telegram channel Boogaloo Intel Drop posted the document "Mujahideen Explosives Handbook" by Abdel Aziz, a well-known jihadist manual that describes the making of IEDs.<sup>51</sup> Criezis notes that during 2019 and 2020 REMVE channels on Telegram showed three types of adopted salafi-jihadist propaganda themes, including instructional manuals, terminology and the use of imagery,<sup>52</sup> with REMVE using and repurposing IS and al-Qaeda imagery, adapting them for their own communication needs and goals.<sup>53</sup>

Islamic State also used cloud-based messaging applications like Telegram to distribute links to propaganda hosted on other sharing platforms including JustPaste.it, Archive.org, Sendvid.com, Dump.to, Woodvid.com and Share.it, in addition to others.<sup>54</sup> It allowed for the creation of what Ayad, Amarasingam and Alexander term the "Cloud Caliphate", a large cache of digital files from IS that aided the curation of "a shared history of the movement".<sup>55</sup> IS's innovative use of sharing platforms and its distribution of site links across multiple messaging applications and social media platforms allowed its propaganda to reach a maximum number of users and increased the time that content remained online before being removed by tech companies or law

47 See Amarnath Amarasingam, "A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit," *CTC Sentinel* 13, no. 2 (2020): pp. 15–19; "Europol and Telegram take on terrorist propaganda online," *Europol* (25 November 2019), <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online>.

48 Meili Criezis, "Remaining and Expanding or Surviving and Adapting? Extremist Platform Migration and Adaptation Strategies," *Global Network on Extremism and Technology* (12 November 2021), <https://gnet-research.org/2021/11/12/remaining-and-expanding-or-surviving-and-adapting-extremist-platform-migration-and-adaptation-strategies/>; Patrick Tucker, "Right-Wing Extremism and Islamic Extremism Spread Online in Similar Ways, New Study Says," *Defense One* (24 August 2020), <https://www.defenseone.com/technology/2020/08/right-wing-extremism-and-islamic-extremism-spreads-online-similar-ways-new-study/167916/>.

49 Naheed Vadsaria and Tucker Holmes, "United States: Radical Groups Using Online Techniques Similar to ISIS," *Babel Street* (12 August 2020), [https://admin.govexec.com/media/08142020\\_us\\_radical\\_groups\\_online.pdf](https://admin.govexec.com/media/08142020_us_radical_groups_online.pdf).

50 *Ibid.*, p. 1.

51 Vadsaria and Holmes, "United States: Radical Groups," p. 2; John Allison, "Terrorism and the IED – Part II," *RUSI* (14 November 2007), <https://rusi.org/publication/terrorism-and-ied-part-ii>.

52 Meili Criezis, "Intersections of Extremism: White Nationalist/Salafi-Jihadi Propaganda Overlap and Essentialist Narratives about Muslims," *Journal of Education in Muslim Societies* 2, no. 1 (2020): pp. 88–96.

53 Ben Makuch and Mack Lamoureux, "Neo-Nazis are Glorifying Osama Bin Laden," *Vice News* (17 September 2019), <https://www.vice.com/en/article/bjwv4a/neo-nazis-are-glorifying-osama-bin-laden>.

54 See Carmen Fishwick, "How a Polish Student's Website Became an ISIS Propaganda Tool," *The Guardian* (15 August 2014), <https://www.theguardian.com/world/2014/aug/15/sp-polish-man-website-isis-propaganda-tool>; Shehabat and Mitew, "Black-Boxing the Black Flag," p. 84.

55 Moustafa Ayad, Amarnath Amarasingam and Audrey Alexander, "The Cloud Caliphate: Archiving the Islamic State in Real-Time," *Institute for Strategic Dialogue and Combating Terrorism Center at West Point* (May 2021): p. iii, <https://www.isdglobal.org/wp-content/uploads/2021/05/Cloud-Caliphate.pdf>.

enforcement. REMVE, in turn, have adopted IS's technique of utilising sharing platforms as well, using cloud-based messaging applications like Telegram to distribute links to sharing platforms such as Archive.org, JustPaste.it, Pastebin.com, Mega.nz, Gofile.io and others.<sup>56</sup> Content including pamphlets, articles, books, manifestos, lists and other material<sup>57</sup> is shared on these sites with the aims of dissemination and increasing its time on the Internet.<sup>58</sup>

When considering the role of cloud-based messaging applications within IS's TTPs and its impact on the TTPs of REMVE, we see a handful of factors come into play. First, the high compatibility with existing communication practices, the low complexity and the low requirement in resources of the technique itself – the change in communication platform – all made adoption simple. Cloud-based messaging platforms are readily available, user friendly and cost-effective. Second, the characteristics of REMVE encouraged such adoption. In a similar fashion to IS, REMVE groups combine a highly centralised core leveraging these applications' secret communication capabilities with a large, dispersed mass of loosely affiliated sympathisers, who rely on the applications' decentralised propaganda dissemination capabilities. The external environment also plays a factor in the adoption of IS TTPs by REMVE since they draw similar benefits in response to similar changes in the external environment. These include staying online as groups come under pressure from public-facing platforms, potentially increasing the time that content stays online by posting and disseminating it across multiple platforms and evading account shutdowns when groups and individuals come under scrutiny from tech companies and law enforcement. Finally, REMVE dissemination of content initially produced by IS demonstrates a familiarity with IS TTPs. Such knowledge of IS TTPs on cloud-based messaging applications was easily accessible either by watching them first-hand (by being embedded in pro-IS channels or chats, as possession of their propaganda material suggests), or simply reading news articles and research reports on IS's online communication TTPs. The adoption of cloud-based messaging applications and of IS's online communication TTPs have benefitted REMVE at a very low cost while increasing their operational range, effectiveness and efficiency.

---

<sup>56</sup> Personal research data.

<sup>57</sup> Ibid.

<sup>58</sup> Interestingly, this technique has also been adopted by opposing groups and movements to further their agendas. A good example of this is the November 2019 Iron March SQL database leak, which included the entirety of IronMarch.org, including registered emails, usernames, public and private posts and the IP addresses of users. This significant doxing effort and data dump was posted by user antifa-data, suggesting a possible link to the Antifa movement or an association with its causes. See Jacques Singer-Emerly and Rex Bray III, "The Iron March Data Dump Provides a Window into How White Supremacists Communicate and Recruit," *Lawfare* (27 February 2020), <https://www.lawfareblog.com/iron-march-data-dump-provides-window-how-white-supremacists-communicate-and-recruit>; "Massive White Supremacist Message Board Leak: How to Access and Interpret the Data," *Bellingcat* (6 November 2019), <https://www.bellingcat.com/resources/how-tos/2019/11/06/massive-white-supremacist-message-board-leak-how-to-access-and-interpret-the-data/>.

## 4 Case Study 2: Unmanned Aerial Vehicles

The use of commercial, off-the-shelf unmanned aerial vehicle or “drone” technology by Islamic State as a central part of its TTPs during its reign in Syria and Iraq was not entirely surprising.<sup>59</sup> Early on, the group distinguished itself for its clever use of this emerging technology both on the battlefield and as an integral part of its propaganda strategy.<sup>60</sup> The adoption of drones by IS followed a significant period of experimentation by other terrorist groups, which sought to leverage this technology’s benefits (identified in 2002 by Christopher Bolkcom as low acquisition costs, potential for high accuracy and operational flexibility, and a variety of purchasing pathways, among others).<sup>61</sup>

Following the 1995 sarin attack in the Tokyo subway by Aum Shinrikyo, the first recorded evidence of a terror plot utilising drones surfaced. The group had previously attempted to distribute sarin using two remote-controlled aircraft, but both crashed during testing. The use of drones by other terrorist groups operating in the Middle East long predated that of IS. Both Hezbollah and Hamas have used this technology with ample frequency, having established medium- to long-term infrastructure dedicated to support such operations. That infrastructure is sufficiently developed to warrant labelling their activities as a “drone programme”.<sup>62</sup> The rapid development of IS’s drone programme, however, distinguishes it from other terrorist programmes.<sup>63</sup> Seven years elapsed between Hezbollah’s initial interest in drones and its first use of them in conflict; IS required only a single year.<sup>64</sup> The pace of this development is all the more remarkable when considering that Hamas and Hezbollah received support from Iran to develop their drone programmes while IS did not.<sup>65</sup>

In their survey of Islamic State drone activities between October 2016 and December 2018, Archambault and Veilleux-Lepage identified three ways in which the group used drones as part of its TTPs. Drones have been used to:

- (1) Conduct strikes by releasing ordnance attached to a drone while it hovered over an intended target. IS began weaponising drones in late 2016 to strike Kurdish Peshmerga soldiers in northern Iraq; armed drones were also deployed against Iraqi army targets during the Mosul campaign and then in fights over eastern Syria in the

59 Marigny Jane Kirschke-Schwartz and Colin Clarke, “How Will Violent Extremists Use Technology in the Future?,” *Global Network on Extremism and Technology* (2 August 2021), <https://gnet-research.org/2021/08/02/how-will-violent-extremists-use-technology-in-the-future/>.

60 Emil Archambault and Yannick Veilleux-Lepage, “Drone Imagery in Islamic State Propaganda: Flying like a State,” *International Affairs* 96, no. 4 (1 July 2020): pp. 955–73, <https://doi.org/10.1093/ia/iiaa014>.

61 “Statement of Christopher Bolkcom Analyst in National Defense Congressional Research Service,” Senate Governmental Affairs Committee Subcommittee on International Security, Proliferation, and Federal Services, Hearing on Cruise Missile Proliferation (2002).

62 Don Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology,” *Combating Terrorism Center at West Point* (October 2016), <https://ctc.usma.edu/app/uploads/2016/10/Drones-Report.pdf>.

63 “Kirschke-Schwartz and Clarke, “How Will Violent Extremists Use Technology in the Future?”.

64 Truls Hallberg Tonnessen, “Islamic State and Technology – A Literature Review,” *Perspectives on Terrorism* 11, no. 6 (2017): pp. 101–11, <https://www.jstor.org/stable/26295959>.

65 Ibid.



second half of 2017.<sup>66</sup> On 24 October 2017, IS utilised a drone to drop two IEDs on a big Syrian army munitions stockpile in the Deir ez-Zor stadium, eventually destroying it.<sup>67</sup>

- (2) Film its military operations, particularly vehicle-borne improvised explosive device (VBIED) attacks and other martyr attacks for propaganda purposes. IS has used drones to document VBIEDs being driven to their targets, their detonations and the aftermath. It has also recorded several drone strikes from the perspective of the drones themselves, using commercial drones, such as the DJI Phantom. Furthermore, drones have been used to film IS executions that then appear in IS propaganda. For example, a 2014 video released by Islamic State's Al-I'tisam media office features footage of IS fighters executing Syrian soldiers at close range and appears to have been taken by a drone.<sup>68</sup>
- (3) Conduct reconnaissance. Videos of reconnaissance flights by a DJI Phantom commercial drone prior to the seizure of the al-Tabqa airfield west of Raqqah, provide an example of drones collecting intelligence. Such reconnaissance flights allowed IS to "check out what the base looked like" and pinpoint critical or susceptible places "before going in with more kinetic strikes", such as using numerous suicide bombers, as Colin Clarke pointed out.<sup>69</sup>

In addition, the drones themselves have also featured in IS propaganda. On several occasions, IS media operatives released propaganda posters on Telegram and other social media platforms featuring digitally altered pictures of drones attacking and destroying United States landmarks, such as the Capitol in Washington D.C. and the Statue of Liberty in New York. In addition, pro-IS Telegram channels have called upon followers to use drones packed with homemade explosives and firebombs to target the group's enemies across the Arab world and the West. For example, one post from 2017 instructed sympathisers that "whoever can buy a drone that [is] able to carry a bottle of firebomb" could easily "burn a factory... police car... fuel tanks... storages... Mol [sic: mall]... electricity facilities." A similar Arabic language message on Telegram suggested additional targets, including churches, newspaper headquarters and broadcasting towers, and asked supporters of the group to disseminate the post on social media.<sup>70</sup>

In addition to encouraging their supporters to conduct drone attacks, IS also disseminated several detailed how-to guides, instructing their sympathisers as to which commercial drones to purchase and which to avoid, how to perform several types of modifications including disabling the recording feature and increasing the range, and how to fabricate

---

66 Don Rassler, "Remotely Piloted Innovation".

67 "Footage Shows Islamic State Drone Blowing up Stadium Ammo Dump," *ABC News* (25 October 2017), <https://www.abc.net.au/news/2017-10-25/footage-shows-is-drone-attack-on-syrian-government-stadium/9085750>.

68 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), <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>.

69 Yasmin Tadjdeh, "Islamic State Militants in Syria Now Have Drone Capabilities," *National Defense* (28 August 2014), <http://www.nationaldefensemagazine.org/articles/2014/8/28/islamic-state-militants-in-syria-now-have-drone-capabilities>.

70 "Private Pro-ISIS Telegram Channel Promotes Use Of Weaponized Drones Against Targets In West," *MEMRI* (16 February 2017), <https://www.memri.org/jttm/private-pro-isis-telegram-channel-promotes-use-weaponized-drones-against-targets-west>.

a rudimentary drone-mounted ordinance delivery system. These guides were disseminated both on Twitter and Telegram and remain available on JustPaste.it as of the time of writing.

Despite the existence of clear pathways for knowledge transfer with regard to drone use both in the form of “vicarious” and “descriptive” transfers, the adoption of drone technologies within the TTPs of REMVE has been rather limited. In fact, drone technologies have only featured in the TTPs of these groups in two rather rudimentary ways: for creating propaganda and for conducting surveillance prior to attacks. Meanwhile, the more complex weaponised drones have not yet been adopted by REMVE. In other words, drone technology appears to be integrated as stand-alone units rather than into broader TTPs leveraging drones for larger operations.

In recent years, drones have been used to film propaganda by REMVE. In 2019, a group claiming to be part of the Atomwaffen Division released a video entitled “Feuernacht”, which showed a group of men burning a Tanakh, a Koran, a book on critical theory and an LGBT pride flag.<sup>71</sup> Part of the video appeared to have been filmed using a drone-mounted camera.<sup>72</sup> While the video’s slick production values might remind a viewer of propaganda videos released by IS, it is unclear whether the use of drones in the product is a deliberate attempt at mimicking the aesthetics of IS’s propaganda products<sup>73</sup> or simply the product of drone-assisted cinematography having become widely diffused throughout society. REMVE drone videography has not yet reached the scale, sophistication or dissemination characteristics of IS’s drone media productions.

Drone technology has also been used for tactical purposes. For example, during the 2017 Charlottesville Unite the Right rally, organisers filmed the infamous night-time tiki torch procession into Lee Park using a drone and released the footage online.<sup>74</sup> Similarly, US Capitol Police have said that high-ranking members of the Oath Keepers attempted but failed to launch a drone with a camera for reconnaissance purposes during the United States Capitol attack in 2021.<sup>75</sup> The highest profile instance of drone use by an REMVE is that of Brenton Tarrant, who flew a small commercial drone over the Al Noor Mosque in Christchurch, New Zealand, “recording an aerial view of the masjid grounds and buildings” focusing on “entry and exit doors, as well as the alleyway where he parked” on the day of the attack.<sup>76</sup> Tarrant’s use of a drone to conduct aerial reconnaissance gives credence to a growing body of anecdotal evidence that REMVE are increasingly beginning to adopt commercial drone technology.<sup>77</sup>

71 “Extremist Content Online: ISIS Issues Threats In Spain, Iraq,” *Counter Extremism Project* (19 November 2019), <https://www.counterextremism.com/press/extremist-content-online-isis-issues-threats-spain-iraq>.

72 “Extremist Content Online”; Argentino, Maher and Winter, “Violent Extremist Innovation”.

73 Marc-André Argentino, Amarnath Amarasingam and Emmi Conley, “One Struggle: Examining Narrative Syncretism between Accelerationists and Salafi-Jihadists,” *International Centre for the Study of Radicalisation* (2022), <https://icsr.info/wp-content/uploads/2022/01/ICSR-Report-One-Struggle-Examining-Narrative-Syncretism-between-Accelerationists-and-Salafi%E2%80%91Jihadists.pdf>.

74 “Independent Review of the 2017 Protest Events in Charlottesville, Virginia” (Hunton & Williams LLP, 24 November 2017), <https://www.policinginstitute.org/wp-content/uploads/2017/12/Charlottesville-Critical-Incident-Review-2017.pdf>.

75 Charles P. Pierce, “These New Details About the ‘Peaceful Tourists’ Who Visited the Capitol Are Incredibly Dark,” *Esquire* (19 January 2022), <https://www.esquire.com/news-politics/politics/a38817339/oath-keepers-january-6-drone-quick-reaction-force/>.

76 “Ko Tō Tātou Kāinga Tēnei, Report: Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain on 15 March 2019,” *The Royal Commission* (2 December 2020), <https://christchurchattack.royalcommission.nz/the-report/>.

77 Yannick Veilleux-Lepage, Chelsea Daymon and Amarnath Amarasingam, “The Christchurch Attack Report: Key Takeaways on Tarrant’s Radicalization and Attack Planning,” *ICCT Perspective* (December 2020).

Despite the use of weaponised drones by REMVE being limited so far, the movement is not blind to the possibilities afforded by drones. As Argentino and his collaborators remarked, REMVE communities online have “shared several blueprints for 3D-printed drone components that ... are meant to enable the home production of weaponized [drones].”<sup>78</sup> In one such video, a remote-controlled handgun is shown mounted on a 3D printed drone.<sup>79</sup> Interestingly, the inspiration for this contraption is most likely not IS (or another terrorist organisation, for that matter), but rather firearm and drone hobbyists who have a long track-record of mounting various firearms on commercial drones, including machine guns and flamethrowers,<sup>80</sup> and posting videos of their exploits on YouTube.<sup>81</sup>

While the drone-mounted firearm was not inspired by IS's TPPs, there is evidence that REMVE communities online are keenly aware of these TPPs. Having surveyed over two hundred REMVE channels on Telegram and image boards such as Endchan and 8kun, Haugstvedt found that while users discussed and shared videos of weaponised drone use in the Middle East, they did not discuss how to construct such drones.<sup>82</sup> In other words, the transfer of knowledge related to weaponised drones in REMVE communities online was limited to vicarious transfer rather than descriptive transfer.

While weaponised drones have not yet been employed by REMVE, it is important to mention that Tarrant pushed for the assassination of high-profile politicians. Chillingly, Argentino warns that this might serve as the catalyst for the adoption of this technique by REMVE, who have a “tendency to emulate past ‘heroes’ or ‘saints’”, with Tarrant being “one of the most influential” of them.<sup>83</sup>

The relative disinterest of REMVE in weaponised drone usage so far, therefore, can be explained by the three aspects of the framework presented in this report. First, the high complexity and cost of establishing a comprehensive drone programme, which did not deter IS, which had easy access to weapons, funds, supply chains and bases, is proving a substantial impediment to REMVE. Furthermore, REMVE privilege tried-and-tested, low-cost techniques that have already proven compatible with their movement, such as mass shootings<sup>84</sup> and vehicle ramming attacks.<sup>85</sup> Second, the lack of one unified REMVE group and the relative decentralisation of the broader movement exacerbates these logistical challenges, while constituencies and goals differ significantly from IS's objective of “flying like a state”.<sup>86</sup> Finally, while vicarious knowledge transfer of IS's TPPs has been observed by Haugstvedt, the lack of descriptive knowledge transfer precluded any wholesale adoption of Islamic State's TPPs.<sup>87</sup>

78 Argentino, Maher and Winter, “Violent Extremist Innovation,” p. 19.

79 Ibid.

80 James Vincent, “Watch This Apparently Legal Drone Fire a Handgun,” *The Verge* (16 July 2015), <https://www.theverge.com/2015/7/16/8976337/drones-quadcopters-handguns-legal>.

81 Cyrus Farivar, “Man Who Built Gun Drone, Flamethrower Drone Argues FAA Can't Regulate Him,” *Ars Technica* (6 September 2016), <https://arstechnica.com/tech-policy/2016/06/man-who-built-gun-drone-flamethrower-drone-argues-faa-cant-regulate-him/>.

82 Håvard Haugstvedt, “The Right's Time to Fly?,” *The RUSI Journal* 166, no. 1 (2 January 2021): pp. 22–31, <https://doi.org/10.1080/03071847.2021.1906161>.

83 Argentino, Maher and Winter, “Violent Extremist Innovation,” p. 20.

84 Graham Macklin and Tore Bjørgo, “Breivik's Long Shadow? The Impact of the July 22, 2011 Attacks on the Modus Operandi of Extreme-Right Lone Actor Terrorists,” *Perspectives on Terrorism* 15, no. 3 (2021): p. 23.

85 Yannick Veilleux-Lepage, “The Extreme Right's Legitimation of Vehicle Ramming,” in *Tracking the Rise of the Radical Right Globally*, William Alchorn (ibidem Press, 2019): pp. 305–8.

86 Archambault and Veilleux-Lepage, “Drone Imagery in Islamic State Propaganda”.

87 Haugstvedt, “The Right's Time to Fly?”.

## 5 Case Study 3: Social Media Bots

Extremist actors have embraced the use of bot technology to disseminate propaganda, expand their reach and, in the case of IS, offer the illusion of a greater following on social media platforms than they have in reality. Bots and AI base text generators – automated software applications emulating or replacing human action – are used by extremists, among others, to amplify ideologies, spread false news, promote likeminded posts, share content and game algorithms by mimicking human activity online.<sup>88</sup>

Islamic State's use of bot technology on Twitter has been well documented.<sup>89</sup> Berger and Morgan have demonstrated IS's utilisation of bot technology to automate tweets and increase followers of IS-related accounts through the usage of third-party services that sell followers.<sup>90</sup> During Berger and Morgan's research, one account amassed almost 100,000 followers instantaneously through this technique.<sup>91</sup> Additionally, small clusters of bots were employed by IS to disseminate tweets, hashtags and propaganda so that if one account were to be suspended, other bot accounts in the cluster could continue to publish content.<sup>92</sup> During their analysis, Berger and Morgan witnessed thousands of accounts using this technique.<sup>93</sup>

Another way bot technology was harnessed by IS supporters was through the development of a Twitter application called The Dawn of Glad Tidings, which attracted users in mid-2014.<sup>94</sup> The application allowed users to stay up to date on news and events about IS while also asking for users' personal account data, enabling the application to post content on their personal Twitter accounts.<sup>95</sup> This technique enabled the widespread dissemination of IS's propaganda while evading Twitter's spam-detection algorithm.<sup>96</sup> During 2014, the app was also available to download off Google Play, making it easily accessible to those who wanted to find it.<sup>97</sup> More recently, on Telegram, IS and its supporters have used third-party bot applications, enabling them automatically to post content, share news, distribute links, engage with users and create archives of content, among other

88 Lisa-Maria Neudert, "Future Elections May be Swayed by Intelligent, Weaponized chatbots," *MIT Technology Review* (22 August 2018), <https://www.technologyreview.com/2018/08/22/104087/future-elections-may-be-swayed-by-intelligent-weaponized-chatbots/>.

89 See J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World* (March 2015), [https://www.brookings.edu/wp-content/uploads/2016/06/isis\\_twitter\\_census\\_berger\\_morgan.pdf](https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf); J. M. Berger and Heather Perez, "The Islamic State's Diminishing Returns of Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters," *The Program of Extremism* (February 2016), <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/JMB%20Diminishing%20Returns.pdf>.

90 Berger and Morgan, "The ISIS Twitter Census".

91 *Ibid.*, p. 32.

92 *Ibid.*; Leanna Garfield, "ISIS has Created Thousands of Political Bots – and Hacktivists Want You to Destroy Them," *Business Insider* (14 December 2014), <https://www.businessinsider.com/anonymous-battles-isis-political-bots-2015-12>.

93 Berger and Morgan, "The ISIS Twitter Census," p. 25.

94 *Ibid.*

95 *Ibid.*; Garfield, "ISIS has Created Thousands of Political Bots".

96 See J. M. Berger, "How ISIS Games Twitter," *The Atlantic* (16 June 2014), <https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/>; Veilleux-Lepage, "Paradigmatic Shifts in Jihadism": p. 36.

97 "ISIS Official App Available to Download on Google Play," *ITV News* (17 June 2014), <https://www.itv.com/news/2014-06-17/isis-official-app-available-to-download-on-google-play>.

automated tasks. For instance, in October 2020, an IS news account on Telegram urged users to contact its bot for access to Islamic State news and links,<sup>98</sup> while various link aggregator channels used bot technology to post identical links at the same time across multiple Telegram channels.<sup>99</sup> These are common ways that bots are used on Telegram by IS and its supporters. Moreover, Telegram is well aware of terrorists' use of its platform, including the use of bot technology. Telegram's @ISISWatch channel, which provides daily reports on banned terrorist content, claims to have banned 2,334 terrorist bots and channels on the platform between 1 and 5 April 2022.<sup>100</sup>

There is, however, much less evidence of REMVE using bot technology to disseminate content to the extent that IS has. Bots have been used by such conspiracy-aligned communities as QAnon to spread false news and information, to promote misinformation about the coronavirus pandemic and to propagate political discourse by right-wing and left-wing communities online.<sup>101</sup> Additionally, there is some evidence of REMVE using bot technology on Telegram to aid in the vetting processes of members and to erase content off channels as a means of reducing its duplication.<sup>102</sup> However, there seems to be less of an adoption of this technology as a whole by organised REMVE groups.

Thus, while both Islamic State and REMVE face a similar set of technique-specific incentives (ease of use, low resource cost) and constraints (repression by communication platforms) for their use of bot technology, group characteristics may play a part in explaining the lack of bot adoption by REMVE. IS's stated goal to create a state provided clear incentives for employing bots to give the impression of a large following, widespread enthusiasm online and a state-like public image.<sup>103</sup> As Khawaja and Khan describe, IS sought "to formulate a media policy" with the intent of reaching the "maximum number of audience [*sic*] with minimum cost and time".<sup>104</sup> Utilising bot technologies aided in these pursuits. Although REMVE groups also aim to reach substantial audiences, there appears to be less of an explicit need to do so on their parts.

Furthermore, since Islamic State is a designated terrorist organisation in most Western countries and many REMVE groups are not, REMVE have benefitted from somewhat more permissive external environments. The absence of designation status as proscribed terrorist entities has allowed some REMVE groups greater freedoms to communicate online which has also resulted in accounts and

98 Author data, Telegram post of Nasr News account (25 October 2020).

99 Author digital ethnography observations; see also Clifford and Powell, "Encrypted Extremism," p. 18.

100 @ISISWatch, Telegram.

101 See Hannah Gais and Megan Squire, "How an Encrypted Messaging Platform is Changing Extremist Movements," *Southern Poverty Law Center* (16 February 2021), <https://www.splcenter.org/news/2021/02/16/how-encrypted-messaging-platform-changing-extremist-movements>; E. J. Dickson, "Nearly Half of Coronavirus Conspiracy Theories on Twitter are Coming from Bots," *Rolling Stone* (22 May 2020), <https://www.rollingstone.com/culture/culture-news/coronavirus-conspiracy-theories-twitter-bots-1004328/>; and Emilio Ferrara, "On Twitter, Bots Spread Conspiracy Theories and QAnon Talking Points," *The Conversation* (28 October 2020), <https://theconversation.com/on-twitter-bots-spread-conspiracy-theories-and-qanon-talking-points-149039>.

102 Gais and Squire, "How an Encrypted Messaging Platform".

103 Ayse Deniz Lokmanoglu, "Coin as Imagined Sovereignty: A Rhetorical Analysis of Coins as a Transhistorical Artifact and an Ideograph in Islamic State's Communication," *Studies in Conflict & Terrorism* 44, no. 1 (2 January 2021): pp. 52–73, <https://doi.org/10.1080/1057610X.2020.1793458>.

104 Asma Shakir Khawaja and Asma Hussain Khan, "Media Strategy of ISIS," *Strategic Studies* 36, no. 2 (2016): p. 104.

content staying online longer.<sup>105</sup> Therefore, one can argue that REMVE have had less of a need to use this TTP due to the liberties they have had online. However, recent years and political developments (notably the attack on the US Capitol on 6 January 2021) have led to stricter moderation and scrutiny and the wholesale deletion of REMVE content by social media platforms. As a result, it is possible that REMVE groups will react in the near future to environmental pressures in a manner similar to that of IS.<sup>106</sup>

---

<sup>105</sup> See David Ingram and Joseph Menn, "Internet Firms Shift Stance, Move to Exile White Supremacists," *Reuters* (17 August 2017), <https://www.reuters.com/article/us-virginia-protests-tech/internet-firms-shift-stance-move-to-exile-white-supremacists-idUSKCN1AW2L5>; Matthew Mosk and Mark Osborne, "Facebook Takes Down Proud Boys, American Guard Accounts Connected to Protests," *ABC News* (16 June 2020), <https://abcnews.go.com/US/facebook-takes-proud-boys-american-guard-accounts-connected/story?id=71286604>; and Jonathan Lewis, "Facebook's Disruption of the Boogaloo Network," *Global Network on Extremism and Technology* (5 August 2020), <https://gnet-research.org/2020/08/05/facebooks-disruption-of-the-boogaloo-network/>.

<sup>106</sup> Mark Scott, "Fringe Social Media Networks Sidestep Online Content Rules," *Politico* (25 January 2022), <https://www.politico.eu/article/fringe-social-media-telegram-extremism-far-right/>.





## 6 Conclusion

This report has presented a theoretical framework that identifies several factors that may propel or hinder a terrorist group's adoption of new TTPs. In doing so, it has identified three main categories of factors that influence how extremist groups learn: technical factors, group factors, and knowledge-transfer factors. Considering these three types of factors can explain why groups adopt or refrain from adopting certain TTPs associated with ideological adversaries. Techniques that work well for one group in a given environment may not work in another ideological, geographical and cultural setting; conversely, TTPs developed in a specific milieu can easily be repurposed by an ideologically different group with little modification if the technical, group and knowledge-transfer characteristics align.

This report presented three scenarios of knowledge transfer and inter-group TTP adoption between IS and Western REMVE. The transition to cloud-based messaging applications shows clear signs of REMVE learning from and adopting IS's practices. Faced with similar environmental constraints and group dynamics, and with clear knowledge exchange mechanisms, REMVE adopted IS's communication and propaganda practices. However, the employment of UAVs saw limited adoption by REMVE, in ways that were not integrated into broader TTPs, unlike IS. Despite vicarious learning channels being available, REMVE found themselves in different environments with differing group constituencies and goals and did not pursue highly complex and resource-intensive techniques,<sup>107</sup> especially as low-cost, low-resource, tried-and-tested techniques, such as mass shootings, had already proven compatible with REMVE ideology. Finally, where IS's extensive use of unaffiliated sympathisers interacting with bots allowed the group to survive in a hostile online environment, the relative impunity of REMVE propaganda online manifested itself in a disinterest for bot use, at least until now.

---

<sup>107</sup> As noted above, the distinctive feature of IS's use of drones lies in its intensive development, modification and videography, which distinguished it from low-cost, easy, hobbyist drone use.



# Policy Section

*This policy section has been written by Inga Kristina Trauthig, Research Fellow, and Amarnath Amarasingam, Senior Research Fellow, at the International Centre for the Study of Radicalisation (ICSR) at King's College London. It provides policy recommendations and is produced independently by ICSR. Recommendations do not necessarily represent the views of the report authors.*

The key findings of this report carry corresponding policy implications for technology companies as this report provides empirical analysis on inter-group learning and adaptation, including some scenario planning with implications for policy adaption based on threat assessments. At the same time, governments around the world are well aware that terrorists have been able to exploit emerging technologies in order to increase their reach – with that increasing their threat potential. The report's comparative analysis identifies a framework that includes a number of factors playing important roles as to whether a group will choose to adopt another's TTPs; such a framework might help to identify avenues of terrorist exploitation of emerging technologies across the ideological spectrum. The following section seeks to achieve a threefold aim: first, to deliver concrete policy recommendations for governmental stakeholders; second, to outline policy options and strategic foresight for technology companies; and, finally, in hand with [1] and [2], to serve as a reference point for a future evaluation of tech policies in order to assess dos and don'ts of technology legislation.

With this, the policy section ensures that the Global Network on Extremism and Technology (GNET), the academic research arm of the Global Internet Forum to Counter Terrorism (GIFCT), is academically advising and supporting technology companies and policymakers on how better to understand the ways in which terrorists are using information technology. This is designed to fulfil not only GIFCT's pillar of learning, but ultimately to improve prevention and responses to terrorist and violent extremist attacks.

## 1. Focus: Policymakers

The outlined factors that facilitate not only passive learning, but also active adaptation of terrorist groups' behaviours raise relevant points that should be addressed and factored in by governmental stakeholders in charge of keeping their societies safe. In addition, national politicians and international and regional policymakers, especially security policymakers and stakeholders working on counterterrorism policies, could take note and consider incorporating the results of this analysis when discussing prioritisation of disruption efforts in particular.

- As this report has outlined, understanding potential push and pull factors for certain technologies, such as cloud-based messaging applications, for instance, is important for disrupting terrorists' successes. This necessity is two-fold: first, encrypted messaging apps offer more protected spaces for communication and can

offer an avenue to share practical guidance on the conduct of terrorist attacks; second, these apps still share some platform features that allow malevolent actors to reach a large number of people and hence propagate and spread their messages to a potentially critical mass, especially when employing bots. Hence the ways in which these two dynamics play out should be monitored and potential ways for disruption identified.

- Furthermore, this report has been particularly insightful in that it outlined existing knowledge transfer or adaptation of cloud-based applications, drones and bot technology. Therefore, the report's insights on the interplay of external environmental factors and internal group deliberations on advantages and disadvantages are relevant for policymakers as these factors can predict a likelihood of adaptation of (certain) technologies by (certain) groups. Law enforcement should aim to undertake holistic assessments bringing together both in-group features and environmental factors to monitor and disrupt terrorist activity efficiently.
- The report also mentions how not every (non-)adoption of an emergent technology can be explained by the group's deliberations; instead circumstantial factors are affecting potential causation. For policymakers this indicates the need for keeping an open mind and aiming to understand the flexibility of terrorist actors when pursuing their aims. In practice, this means seeking exchange with the research community and practitioners working on deradicalisation programmes in order to understand some of the unpredictable dynamics guiding some groups and individual extremists.

## 2. Focus: Technology Companies

In addition to the report findings and their implications for political stakeholders, the analysis is also relevant for technology companies aiming to rein in the exploitation of their platforms for malevolent purposes, including emergent technologies.

- The main policy implication of this report is the pressure on technology companies to work towards disrupting the transfer of knowledge so that extremists have fewer opportunities to learn from other groups and exploit access to emerging technology know-how. In addition to directly targeting and taking down extremist content, this report also outlined how removing instructions produced by non-ideologically minded individuals that can assist terrorist groups to weaponise a given technology might be necessary.
- Furthermore, the report has shown how platform features or intrinsic characteristics of emergent technologies, such as ease of use or availability, are a catalyst for adoption. This indicates the necessity for intra-company exchange and deliberations, such as teams focused on investigations or threat intelligence with developers, in order to communicate early potential avenues of exploitation by extremists.

- Finally, one significant takeaway is the reliance of both IS and REMVE on sharing platforms, using cloud-based messaging applications such as Telegram to distribute links to Archive.org, JustPaste.it, Pastebin.com, Mega.nz and Gofile.io. This finding emphasises the importance of cooperation and exchange between bigger and smaller tech firms in order to find the right balance between tackling illegal and harmful content and maintaining liberties online.

### 3. Focus: Strategic Foresight and Broader Implications

In addition to the policy recommendations derived directly from the above report, broader implications and strategic deliberations are also evident from this study regarding how racially and ethnically motivated violent extremists embrace and mimic Islamic State's use of emerging technologies.

- This GNET report has outlined the adaptation by some of IS's TTPs with regard to cloud-based applications, bots and drones by REMVE. However, there is a qualitative difference between these actors, as pointed out by the report authors themselves. IS, designated a terrorist group almost throughout the world, found itself facing ongoing crackdowns by social media companies during its pursuit to promote its version of a state to as many sympathisers as possible. The most pressing big-picture question is how the relative permissibility of the online environment for REMVE content has diminished the push factors towards some emergent technologies, such as the reliance on bots. In the future these external factors, adding to the push and pull factors for specific groups and individuals, are likely to change.





### CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR  
King's College London  
Strand  
London WC2R 2LS  
United Kingdom

T. **+44 20 7848 2098**  
E. **[mail@gnet-research.org](mailto:mail@gnet-research.org)**

Twitter: **[@GNET\\_research](https://twitter.com/GNET_research)**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at [www.gnet-research.org](http://www.gnet-research.org).

© GNET