TATuP Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis
Journal for Technology Assessment in Theory and Practice

oekom science

RESEARCH ARTICLE

The paradox of progress: How 'disruptive,' 'dual-use,' 'democratized,' and 'diffused' technologies shape terrorist innovation

Don Rassler*,[1], Yannick Veilleux-Lepage[2]

Abstract • Building upon the existing literature on terror innovation, this research article introduces a new analytical framework that highlights four key elements of emerging technologies which facilitate their adoption by terrorist groups. We posit that technologies that are inherently 'disruptive,' 'dual-use,' 'democratized,' and 'diffused' are particularly susceptible to misuse by terrorists, and that it is the interplay between these factors that helps to drive future directions of tech-enabled terror. We draw on terror and extremist interest in and use of two key technology areas – unmanned aerial systems and additive manufacturing, specifically 3-D-printed firearms – as examples to highlight how the factors in the framework interact and how they help to drive innovative terror behavior. We conclude with a series of concise recommendations to mitigate harmful terrorist use of these and other disruptive technologies and limit the impact of future tech-enabled terrorist innovations.

***Das Paradox des Fortschritts**: Wie ‚disruptive', ‚Dual-Use-', ‚demokratisierte' und ‚verbreitete' Technologien die Innovation im Bereich des Terrorismus prägen*

Zusammenfassung • *Aufbauend auf der bestehenden Literatur zu Terrorinnovationen wird in diesem Forschungsartikel ein neuer Analyserahmen vorgestellt. Dieser hebt vier Schlüsselelemente emergenter Technologien hervor, die deren Übernahme durch terroristische Gruppen erleichtern. Wir gehen davon aus, dass Technologien, die von Natur aus ‚disruptiv', ‚dual-use', ‚demokratisiert' und ‚verbreitet' sind, besonders anfällig für terroristischen Missbrauch sind, und dass das Zusammenspiel dieser Faktoren die künftige Richtung des technologiegestützten Terrors mitbestimmen wird. Anhand des Interesses von Terroristen und Extremisten an zwei Schlüsseltechnologien – unbemannte Flugsysteme und additive Fertigung, insbesondere 3-D-gedruckte Schusswaffen – zeigen wir auf, wie die verschiedenen Faktoren des Analyserahmens zusammenwirken und wie sie dazu beitragen, innovatives Terrorverhalten zu fördern. Wir schließen mit einer Reihe von Empfehlungen, um die terroristische Nutzung dieser und anderer disruptiver Technologien einzudämmen und die schädlichen Auswirkungen künftiger technologiegestützter terroristischer Innovationen zu begrenzen.*

Keywords • *terrorist innovation, emerging technologies, unmanned aerial systems, additive manufacturing*

This article is part of the Special topic "Malevolent creativity and civil security: The ambivalence of emergent technologies," *edited by A. Gazos, O. Madeira, G. Plattner, T. Röller, and C. Büscher. https://doi.org/10.14512/tatup.33.2.08*

Introduction

Terrorist groups 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 (Veilleux-Lepage et al. 2022). To gain such an advantage, violent non-state actors routinely experiment with new or emerging technologies (Cronin

* *Corresponding author: don.rassler@westpoint.edu*
[1] *Combating Terrorism Center, U.S. Military Academy at West Point, West Point, US*
[2] *Royal Military College of Canada, Kingston, CA*

https://doi.org/10.14512/tatup.33.2.22
Received: 15. 01. 2024; revised version accepted: 08. 04. 2024;
published online: 28. 06. 2024 (peer review)

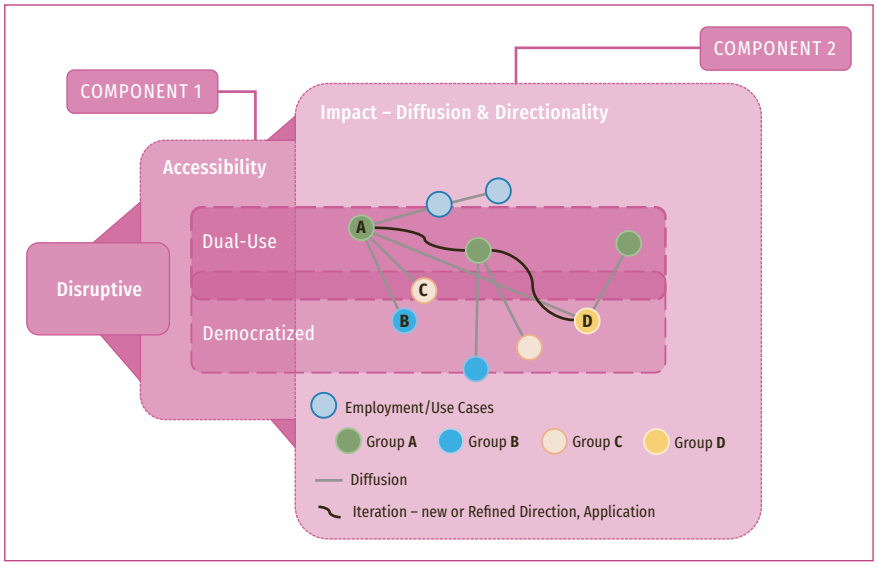


Figure 1: Framework – the four 'D' factors shaping terror innovation.
Source: authors' own compilation

2020). Two key disruptive technology areas that terror and extremist networks and movements have been heavily interested in, experimented with, and have used (or attempted to use) in innovative operational ways for the past decade, are unmanned aerial systems (UAS) and additive manufacturing specifically 3-D-printed firearms (3DPF) (Basra 2023; Chávez and Swed 2021; Rassler 2016; Veilleux-Lepage 2021; Veilleux-Lepage and Archambault 2022). As a result, these two technology areas provide important insights into how terrorists and extremists approach new technologies and the process and factors that help to shape innovative terror use of them. While terrorist groups must continuously innovate, the decision to leverage new technologies, nonetheless, presents an important paradox for terrorist organizations. Leveraging new technology is inherently a risky endeavor and doing so involves a cost-benefit judgment that might prove to be incorrect. Moreover, groups' efforts to adopt a new technology might fail for a variety of reasons and thus the group would pay the costs associated with experimenting with a new technology without reaping any of the anticipated benefits (Cragin et al. 2007; Veilleux-Lepage 2020). Terrorists and extremists also confront risks and costs when choosing not to adopt new technologies or innovate. They must find ways to strike a balance in making these decisions. This is because terror groups and movements who fail to innovate will either "be degraded to the point of irrelevance" or fail to attract resources, recruits and supporters (Gartenstein-Ross et al. 2019, p. 10). Building on the existing literature on terrorism innovation (Cragin et al. 2007; Dolnik 2007; Gartenstein-Ross and Joscelyn 2022; Lubrano 2021; Veilleux-Lepage 2020; Veilleux-Lepage et al. 2022), this article discusses how two key technologies – additive manufacturing and UAS – are currently or may in the future be leveraged by violent non-state actors by introducing a novel framework designed to showcase how the interplay and interrelationship between four 'D' factors – dual-use, democratized, diffuse, and directionality – help drive how extremists and terrorists use disruptive technologies. In doing so, this article highlights why these types of technologies, and other related technologies, warrant care and scrutiny. The article concludes with a series of short recommendations to mitigate harmful future terror use of key technologies and curb future, related terrorist innovations; these are aimed at law enforcement and intelligence agencies, domestic and international regulators, and commercial manufacturers.

Technology and the interplay of terror innovation

Terrorists and extremists can leverage a wide range of technologies to harm, achieve or enhance another desired effect, and/or to innovate. Disruptive technologies like additive manufacturing, UAS, and generative artificial intelligence, which have the potential to revolutionize entire industries or fields of science, and society generally, are particularly attractive as they hold the same potential and promise for extremists and terrorists too. As such, it is unlikely that these technologies will become contained. To use the words of noted Standford University bioethicists, "the centaur has left the barn" (Dowd 2005, para. 6).

The framework introduced in this article highlights how key accessibility factors interplay with one another and the influence and bearing these factors have on other important impact variables, which in turn help to drive both incremental and radical innovations by violent non-state actors. The framework is not designed to offer insights into *why* terrorists and extremists do or do not make innovative use of technologies, and the variables, tradeoffs, and decisions that violent non-state actors must navigate in evaluating whether to adopt a specific innovation or

technology. Instead, the framework offers a visual and conceptual perspective to help researchers and practitioners to understand how terror innovation and technology-related terror threats evolve as part of an interactive system. The framework, visually portrayed in Figure 1, is designed to showcase the interrelationship between four 'D' factors – dual-use, democratized, diffusion, and directionality – and how they interact and shape terror innovation.

The following two sections introduce the two main components of the framework. Examples of terror and extremist interest in and operational use of UAS and 3DPF are provided in both sections to highlight the applicability of the framework.

Accessibility – dual-use and democratized

The open-source technological revolution that Cronin (2020) describes is having a broadly disruptive impact on the tools, knowledge, and tradecraft available to state and non-state actors. The first component of the framework (Figure 1) highlights how this ongoing change in the accessibility of key technologies and information, and ways to share data, is helping state and non-state parties to enhance and diversify their capabilities, to develop new capabilities, and to innovate.

This change in accessibility has been principally shaped by the interplay between two key, interrelated factors: 1) dual-use items – products, software, and technologies designed for civilian purposes but can also be adapted for military use and 2) the democratized availability of systems and communication platforms that have made it easier and more efficient for individuals and networks to more securely share knowledge and technical know-how about how to use dual-use items, and to learn from other actors. Both factors continue to lower barriers to entry for non-state actors. Not only has this provided non-state actors with more tools and options to creatively tinker and experiment with, which opens pathways for them to innovate, it also has been shifting power from "dominant players" to other types of "players" (Cronin 2020, p. 7).

The Islamic State's innovative transformation of commercial-off-the-shelf (COTS) drones into airborne munitions-dropping weapons is an important example. For a considerable period, drones were primarily developed by states for military purposes. But, over the past two decades drone technology, and capable commercial UAS have become much more accessible and affordable for the average consumer. The Islamic State recognized this as an opportunity, and it was able to acquire a large fleet of small COTS drones through a global and layered supply chain (Rassler 2018). Then, through some creative tinkering the group quickly developed a fleet of small, easy-and-cheap-to-replicate munition-dropping capable drones; a Do-It-Yourself air force (Rassler 2018). For several months, the only effective solution to the Islamic State's new weaponized drones was small arms fire (Larter 2017).

While the Islamic State's creative weaponization of a dual-use item (i.e. commercial drones) led to its initial breakthrough innovation, the legacy of the group's innovation is tied to how its simple modifications – the know-how or playbook for how it weaponized its drones – was democratized, widely publicized, and shared around the world. Both elements, the use of a dual-use item and the democratized sharing of innovation know-how, and the interplay between those two factors, have facilitated the diffusion of munition-dropping commercial drones as a new method to attack for different types of actors. For example, a wide range of actors – from Mexican drug cartels to Iranian proxies and state militaries, have been inspired by, have leveraged, and in some cases have sought to improve upon and take in new directions, the Islamic State's 'drop-a-munition-from-a-commercial-drone' idea. The fact that the Ukrainian and Russian militaries have both used and experimented with munition-dropping drones similar to those used by the Islamic State (Axe 2022; Chapple 2022) illustrates that the learning ecosystem for how dual-use items can be used for harm cuts across states and non-state actors as distinct categories. It is clear that both 'types' of actors are learning lessons from each other, which helps to further diffuse innovative ideas and capabilities, and push those capabilities in new directions.

Over the past two decades drone technology, and capable commercial UAS have become much more accessible and affordable for the average consumer.

Terrorist interest in and attempts to use 3DPF (Veilleux-Lepage 2021) also highlights how dual-use items and democratized knowledge and know-how interact and can be combined to generate new pathways for mal-intended actors to inflict harm. For example, to create a 3DPF, an actor must first acquire or gain access to hardware – an actual 3D printer (i.e. a dual-use commercial good). Today, there are numerous high-quality 3D printers on the market for under $ 1,000 US. A second requirement is software that enables a 3D printer to 'read' a computer-animated design (CAD) file so it can 'print' or physically create the object. Software is thus a category that cuts across the dual-use and democratized categories as concepts, as it can be both a dual-use item (i.e. software that comes pre-loaded on a 3D printer) and can be acquired or shared in more decentralized ways. There is an entire online ecosystem where 3D printing hobbyists share design files and technical know-how, where

technical information is democratized and shared. There are segments of that rich open-source community that support the development of 3DPF, and ensuring that individuals maintain access to information, plans, and software that would allow them independently to produce such weapons. Mainstream tech companies have banned the sharing of CAD files for 3DPF on their platforms (Barton 2019), but a litany of websites and chat servers emerged to fill the void left by these crackdowns (Sorensen 2019). At the same time, plans for 3DPF have evolved and become significantly more sophisticated since they were introduced online in 2013.

Important points of intersection between extremist and online 3DPF communities have emerged, and terrorist interest in the operational use of 3DPF has also increased across time. For example, according to research the creator of "the world's most popular 3-D-printed gun […] the FGC-9" posted extremist messages and "made anonymous threats of violence" online (Basra 2023, executive summary). From 2016 to December 2023, a total of 27 terrorist plots involving 3DPF were disrupted across various countries, illustrating the growing concern over this technology's use in terrorism, and its appeal. The United Kingdom reported the highest number of incidents, with seven cases, while the United States followed with three cases. Other countries also faced such threats.

The timeline of these incidents shows an increasing trend. In 2016, there was just one incident, and 2019 also saw a single case. However, the numbers rose in subsequent years, with three incidents in 2020, six in each 2021 and 2022, and a significant jump to ten incidents in 2023. Among these, some plots were particularly alarming. In October 2019, for example, Stephan Balliet conducted a terrorist attack in Halle, Germany, which he livestreamed. Balliet's arsenal of weapons included a longsword (not used during the attack), pipe bombs and improvised explosive devices, and six firearms – five of which were improvised. While these weapons were mostly constructed out of steel, aluminum, and wood, Balliet used some 3DPF components. According to his manifesto, one of his motivations for the attack was to "prove the viability of improvised weapons" (Koehler 2019, p. 15).

More recently, in 2022, Icelandic authorities arrested four individuals linked to a Neo Nazi terror plot. This group planned to use a combination of semi-automatic and 3DPF to launch attacks on various societal institutions (Boffey 2022). These arrests were part of a larger European operation, leading to police raids in Germany, Italy, Croatia, and Lithuania.

Impact – diffusion and directionality

The second component of the framework (also visually portrayed in Figure 1) involves the inclusion of two other 'Ds' – diffusion and directionality. Diffusion involves "dispersion through a space or over a surface." (OED 2023), whereas directionality can be understood as "relating to direction in space" (MWD 2024). While the previous two 'Ds' – dual-use and democratized – primarily affect the accessibility of equipment, technology, systems, and know-how that is available to state and non-state actors, the diffusion of key innovations, capabilities, and know-how helps to amplify their impact. This in turn – through further iteration by various parties – helps to push technology-related threats in different directions.

The nature of the threats posed by terrorists leveraging these emerging technologies cannot be fully understood by looking at developments in the terrorism sphere alone.

The framework attempts to visually capture the interplay between these four 'D' factors and how they interact and influence each other as part of a system, in two ways. First, is the build character of the framework itself. The two accessibility factors – dual-use and democratized – are core, foundational 'drivers' that guide and make the impact factors of diffusion and directionality more likely. Or put another way, the accessibility factors – due to their open nature – help ideas, tactics, and the development of new weapons or operational approaches to diffuse. This creates an environment where a wide range of actors (i.e., individuals, non-state actors, and states) have an expanded and more diversified pool of diffused materiel and know-how to pull from and to create; a dynamic which broadens opportunity pathways, or directions, an actor can push a threat. The simplest way to characterize the link between the accessibility and impact factors is that more diversified inputs will likely lead to more diversified outcomes.

The state and projections of the global drone market help to highlight these interplay dynamics. In 2021 the global market for COTS UAVs was valued at over 20.8 billion USD, and it is projected to further grow to nearly 1,205 billion USD by 2030 (Straits Research 2021). The global drone market is also "diverse and multifaceted, encompassing various segments" (Beekman 2023). Ongoing advancements and innovations occurring across a range of key technologies, from sensors to powering systems, and data processing capabilities, will also ensure that tomorrow's COTS UAVs will be more capable than they are today.

This means that not only will violent non-state actor use of drones remain a persistent problem and increase in scale, the character of the terror drone threat, and the ways in which it presents itself and directions it takes, will likely become more diversified as well. For example, the majority of COTS UAVs

https://doi.org/10.14512/tatup.33.2.22

available today are powered by lithium-ion batteries, which limit how far and for how long those drones can fly. When viewed through the lens of extremism and terrorism, this limits the range from which a terror entity can conduct a stand-off attack. But, "alternative powering options, such as UAS powered by hydrogen fuel cell technology or hybrid fuel/powering systems (i.e., solar), are already commercially available" (Rassler 2024, p. 5). In the next decade "hydrogen fuel cell and solar UAS technology will evolve and mature, and will also likely become more available to the average consumer, which will make longer ranges more accessible" (Rassler 2024, p. 5). This will open-up new range options, and help to push the terror drone threat in new directions.

The second important takeaway from the framework is that the interplay between the four 'Ds' is hard to box or bound. For example, dual-use and democratized are factors that have an ongoing influence and bearing on the diffusion, or spread, of new innovations and capabilities. As a result, dual-use and democratized are shown as factors that cut across the meta-accessibility and impact categories. The circular employment use cases, linear diffusion paths (blue lines), and curvy iteration courses (black lines) in Figure 1 have been included to help model in a general way how the 4 'D' factors interact and influence one another. For example, theoretical terror Group A (green circle) recognizes the broad availability of commercial UAV quadcopters and decides to acquire several stock quadcopters to conduct surveillance missions and/or to support propaganda. Groups B and C observe that Group A is utilizing commercial quadcopters in these ways, and decide to copy and mirror the idea, highlighting how knowledge related to the use of the dual-use good (i.e., COTS UAV) for those purposes democratized and the tactic diffused.

Group A then decides that it wants to weaponize a commercial quadcopter. As the first curvy black line highlights, Group A experiments until it develops a creative and low-cost way to drop munitions from a UAV; an innovation that pushes the threat in new directions. Groups B and C mirror this new 'drop a munition from a commercial UAV' approach too. Group D, which has been observing all of this activity, iterates on Group's A UAS weaponization approach and develops a way to integrate commercially available crowd counting software, which "utilizes deep learning technology to quickly and accurately analyze live video," (Canon USA 2024) so the group can maximize of the impact, and lethality, of its UAS bombs.

The findings from a comparative study of the drone programs of five-armed non-state actors also help to bring some of these diffusion and directionality considerations to light (Veilleux-Lepage and Archambault 2022). The study found that all five non-state entities used or developed weaponized drones, and that all five have used pilot-to-target as a drone attack modality. So, when looking across the five programs, pilot-to-target was a common drone weaponization feature: a diffused attack method. But that study also found that there were important differences in how each of the five non-state entities used drones. For example, while each of the five groups have used pilot-to-target as a drone weaponization pathway, how each of the five groups have utilized drones in that way has been guided by a group's own preferences (Veilleux-Lepage and Archambault 2023).

The fact that the study found "that there is no single route of development for the use of drones by non-state entities, nor is there a pattern that these groups want to follow in order to expand their capabilities" (Veilleux-Lepage and Archambault 2022, p. 1) highlights why directionality is also an important factor for the framework to consider. Indeed, since "each organization uses drones in a manner that is unique to its own set of logistical, political, and strategic parameters" (Veilleux-Lepage and Archambault 2022, p. 1) considering directionality as a key factor will help practitioners to better anticipate, and be on the look-out for, differences and change.

Even though how different non-state actors use drones, or other disruptive technologies, will vary from group to group or network to network, directionality will still be guided by several primary characteristics that aim to improve operational outcomes. These include characteristics such as surprise and speed, effectiveness and/or efficiency, as well as impact or outcome variables like lethality.

Responses and policy recommendations

Advancements in key technologies and their widespread availability offer significant benefits, yet they also pose risks by providing malevolent actors with new capabilities. The interaction of the four 'D' factors in our framework is a driving force behind the evolution of violent non-state threats.

Law enforcement and intelligence

If not already being done on a broad scale, governments should start systematically cataloging cases of proven interest in, and use of, UAS and additive manufacturing by terrorist actors, as well as innovative ways that private citizens have used these technologies. This data would allow those tracking these threats to quickly identify noteworthy developments and to better understand the evolution of these phenomena. Such cataloguing could initially be implemented and maintained with minimal resources and effort, and it would pay dividends in the years ahead as it would help government officials make more informed resourcing and regulatory decisions.

In addition, the nature of the threats posed by terrorists leveraging these emerging technologies cannot be fully understood by looking at developments in the terrorism sphere alone. For example, evaluating how terrorists might leverage additive manufacturing requires law enforcement and intelligence agencies to pay attention and understand innovative developments that occur in private industry, academia and by creatively minded hobbyists. To stay current, analysts following these issues therefore need to monitor innovations across a number of spheres, and be part terror specialist, part technologist, and part industry expert.

 https://doi.org/10.14512/tatup.33.2.22

The overwhelming majority of game-changing developments in these spheres is taking place in plain sight.

Multinational

A potentially fruitful avenue for international cooperation is the United Nations Security Council Resolution 2325. Unanimously approved, the resolution called upon states to take into account the risks of terrorist groups using "rapid advances in science, technology, and international commerce for proliferation purposes" (Black-Branch 2017, p. 228). In addition, the Resolution also added controlling access to intangible transfers of technology as a new obligation for UN member-states. The Resolution also recognizes the need to continue drawing upon relevant expertise from industry, the scientific community, and academia in order to ensure access to up-to-date information on these technologies and in order to educate these communities about the terrorism challenges at hand.

Commercial

Finally, manufacturers can help counter misuse of emerging technologies by adopting 'Design Against Crime' (DAC) practices. The DAC involves designing products in such a way as to reduce the harmful 'misuse' of emerging technologies (Ekbom 2005). For example, most modern commercially sold photocopiers will automatically recognize banknotes, and either decline to reproduce them or produce a distorted image of them to prevent counterfeiting (Girgensohn et al. 2018).

While promising, DAC initiatives require manufacturers to introduce such features in close coordination with both public authorities and also other manufacturers in order to ensure maximum reliance on common standards and protocols. In addition, manufacturers can also further protect their products from being misused by sharing technical information about future products with regulatory and government agencies.

Conclusion

This article delves into how additive manufacturing and UAS are being, or could be in the near future, exploited by violent non-state actors. It introduces a novel framework to analyze the dynamics of terrorists' use of disruptive technologies, focusing on four key factors: dual-use, democratized, diffused, and directionality. These factors not only drive extremists' use of these technologies but also underline why such technologies demand careful observation and regulation.

The framework presented elucidates how access to technology, shaped by its dual-use nature and democratized availability, enhances the capabilities of state and non-state actors alike. It underscores the lowering of barriers to entry for non-state actors, shifting power dynamics, and factors fostering innovation. Furthermore, the interplay of dual-use and democratized factors not only facilitates the diffusion of these technologies but also influences their directionality – the ways in which they are adapted and evolved for specific purposes. This aspect is vital for understanding and anticipating the evolution of technology-related terror threats.

In the face of these emerging threats, the article proposes targeted recommendations for law enforcement, intelligence agencies, international regulators, and commercial manufacturers. Systematic cataloging of terrorist use of these technologies, cross-sectoral monitoring, and innovative collaborations are crucial.

Funding • This work received no external funding.
Competing interests • The authors declare no competing interests.

References

Axe, David (2022): Ukraine's $ 10,000 drones are dropping tiny bombs on Russian troops. In: Forbes, 13. 04. 2022. Available online at https://www.forbes.com/sites/davidaxe/2022/04/13/ukraines-10000-drones-are-dropping-tiny-cheap-bombs-on-russian-troops/, last accessed on 11. 04. 2024.

Barton, Champe (2019): As social networks crack down, 3d-printed gun community moves to new platforms. In: The Trace 25. 07. 2019. Available online at https://www.thetrace.org/2019/07/3d-printed-guns-social-media-ban/, last accessed on 11. 04. 2024.

Basra, Rajan (2023): Behind the mask. Uncovering the extremist messages of a 3d-printed gun designer. London: International Centre for the Study of Radicalisation. Available online at https://icsr.info/wp-content/uploads/2023/10/ICSR-Report-Behind-the-Mask-Uncovering-the-Extremist-Messages-of-a-3D%E2%80%91Printed-Gun-Designer.pdf, last accessed on 11. 04. 2024.

Beekman, Johannes (2023): Skyward bound. Navigating the evolving terrain of the global drone market. In: IoT Marketing, 15. 12. 2023. Available online at https://iotmktg.com/skyward-bound-navigating-evolving-terrain-of-the-global-drone-market/, last accessed on 11. 04. 2024.

Black-Branch, Jonathan (2017): Nuclear terrorism by states and non-state actors. Global responses to threats to military and human security in international law. In: Journal of Conflict and Security Law 22 (2), pp. 201–248. https://doi.org/10.1093/jcsl/krx004

Boffey, Daniel (2022): Icelandic police arrest four people over alleged terror attack plans. In: The Guardian, 22. 9. 2022. Available online at https://www.theguardian.com/world/2022/sep/22/icelandic-police-arrest-four-people-over-alleged-terror-attack-plans, last accessed on 11. 04. 2024.

Canon USA (2024): Crowd people counter. Available online at https://www.usa.canon.com/shop/p/crowd-people-counter-version-1-0?color=Black&type=New, last accessed on 11. 04. 2024.

Chapple, Amos (2022): The drones of the Ukraine war. In: Radio Free Europe/Radio Liberty, 17. 11. 2022. Available online at https://www.rferl.org/a/ukraine-russia-invasion-drones-war-types-list/32132833.html, last accessed on 11. 04. 2024.

Chávez, Kerry; Swed, Ori (2021): The proliferation of drones to violent nonstate actors. In: Defence Studies 21 (1), pp. 1–24. https://doi.org/10.1080/14702436.2020.1848426

Cragin, Kim; Chalk, Peter; Daly, Sara; Jackson, Brian (2007): Sharing the dragon's teeth. Terrorist groups and the exchange of new technologies. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/MG485

Cronin, Audrey (2020): Power to the people. How open technological innovation is arming tomorrow's terrorists. Oxford: Oxford University Press.

https://doi.org/10.14512/tatup.33.2.22

Dolnik, Adam (2007): Understanding terrorist innovation. Technology, tactics and global trends. London: Routledge.

Dowd, Maureen (2005): What rough beast? In: The New York Times, 07. 05. 2005. Available online at https://www.nytimes.com/2005/05/07/opinion/what-rough-beasts.html, last accessed on 11. 04. 2024.

Ekblom, Paul (2005): Designing products against crime. In: Nick Tilley (ed.): Handbook of crime prevention and community safety. London: Routledge, pp. 203–244. https://doi.org/10.4324/9781315724393

Gartenstein-Ross, Daveed; Joscelyn, Thomas (2022): Enemies near and far. How jihadist groups strategize, plot, and learn. New York, NY: Columbia University Press. https://doi.org/10.7312/gart19524

Gartenstein-Ross, Daveed; Shear, Matt; Jones, David (2019): Virtual plotters, drones, weaponized AI? Violent non-state actors as deadly early adopters. s.l.: Valens Global. Available online at https://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/, last accessed on 11. 04. 2024.

Girgensohn, Andreas; Wilcox, Lynn; Liu, Qiong (2018): Automatic rights management for photocopiers. In: Proceedings of the ACM Symposium on Document Engineering 2018. New York, NY: ACM, pp. 1–10. https://doi.org/10.1145/3209280.3209531

Koehler, Daniel (2019): The Halle, Germany, synagogue attack and the evolution of the far-right terror threat. In: CTC Sentinel 12 (11), pp. 14–20. Available online at https://ctc.westpoint.edu/halle-germany-synagogue-attack-evolution-far-right-terror-threat/, last accessed on 11. 04. 2024.

Larter, David (2017): SOCOM commander. Armed ISIS drones were 2016's 'most daunting problem'. In: Defense News, 16. 05. 2017. Available online at https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/, last accessed on 11. 04. 2024.

Lubrano, Mauro (2021): Navigating terrorist innovation. A proposal for a conceptual framework on how terrorists innovate. In: Terrorism and Political Violence Routledge 35 (2), pp. 248–263. https://doi.org/10.1080/09546553.2021.1903440

MWD – Merriam-Webster Dictionary (2024): "Directionality". Available online at https://www.merriam-webster.com/dictionary/directionality, last accessed on 15. 04. 2024.

OED – Oxford English Dictionary (2023): "Diffusion". Available online at https://www.oed.com/dictionary/diffusion_n?tab=factsheet#6760287, last accessed on 15. 04. 2024.

Rassler, Don (2016): Remotely piloted innovation. Terrorism, drones and supportive technology. West Point, NY: Combating Terrorism Center at West Point.

Rassler, Don (2018): The Islamic State and drones. Supply, scale, and future threats. West Point, NY: Combating Terrorism Center at West Point.

Rassler, Don (2024): Going the distance. The emergence of long-range stand-off terrorism. In: CTC Sentinel 17 (2), pp. 1–10. Available online at https://ctc.westpoint.edu/going-the-distance-the-emergence-of-long-range-stand-off-terrorism/, last accessed on 15. 04. 2024.

Sorensen, Zachary (2019): 3D printed guns and gun control. In: Washington University Political Review, 19. 04. 2019. Available online at https://www.wupr.org/2019/04/19/3d-printed-guns-and-gun-control/, last accessed on 15. 04. 2024.

Straits Research (2021): Commercial drone market growth, analysis. Report to 2022–2030. Pune: Straits Research. Available online at https://straitsresearch.com/report/commercial-drone-market, last accessed on 15. 04. 2024.

UNSCR – United Nations Security Council (2016): Resolution 2325. Non-proliferation of weapons of mass destruction. New York, NY: United Nations. Available online at http://unscr.com/en/resolutions/2325, last accessed on 15. 04. 2024.

Veilleux-Lepage, Yannick (2020): How terror evolves. The emergence and spread of terrorist techniques. Lanham, MD: Rowman & Littlefield.

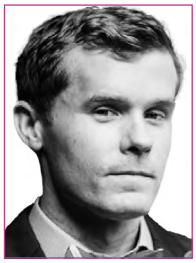
Veilleux-Lepage, Yannick (2021): Ctrl, hate, print. Terrorists and the appeal of 3-D-printed weapons. The Hague: International Centre for Counter-Terrorism – ICCT.

Veilleux-Lepage, Yannick; Archambault, Emil (2022): A comparative study of non-state violent drone use in the Middle East. The Hague: International Centre for Counter-Terrorism – ICCT.

Veilleux-Lepage, Yannick; Archambault, Emil (2023): Étude comparative de l'usage des drones par des groupes armés non étatiques au Moyen-Orient. The Hague: International Centre for Counter-Terrorism – ICCT.

Veilleux-Lepage, Yannick; Daymon, Chelsea; Archambault, Emil (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 and Technology.

Wigmore, Ivy (2017): What is FPV drone (first-person view drone)? In: TechTarget. Available online at https://www.techtarget.com/whatis/definition/FPV-drone-first-person-view-drone, last accessed on 15. 04. 2024.



ASST. PROF. DON RASSLER
is an Assistant Professor in the Department of Social Sciences and Director of Strategic Initiatives at the Combating Terrorism Center (CTC) at the U.S. Military Academy at West Point. His research interests are focused on counterterrorism, how terrorist groups innovate and use technology, and understanding the changing dynamics of militancy in Asia.

ASST. PROF. DR. YANNICK VEILLEUX-LEPAGE
is an Assistant Professor in the Department of Political Science and Economics at the Royal Military College of Canada in Kingston, Ontario. His research focuses on the intersection of technology, far-right extremism, and the evolution of terrorist tactics.