CENTER FOR WAR STUDIES

CSS ETH Zürich

The Vulnerabilities of the Drone Age
Established Threats and Emerging Issues out to 2035

Final Report

Dr James Rogers, Dr Dominika Kunertova

2022

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Key Findings

Over 24-months, the Vulnerabilities of the Drone Age (VDA) project team, led by Dr James Rogers and Dr Dominika Kunertova, gathered evidence from three NATO Science for Peace and Security (SPS) funded Strategic Foresight Analysis workshops to analyse the global proliferation of drones to hostile state and non-state actors. The present report focuses on drone threats posed to NATO Member and Partner Nations and is separated into three sections: 'Drone Attack', 'Drone Defence', and 'Future Threats'. Our findings, summarised below, detail the most concerning vulnerabilities of the drone age:

1 Drone Attack: The Threat from Hostile State and Non-state Drones

- **We have entered a new age of assassinations:** Weaponised drones with ever greater lethality, payload, and range are increasingly being used in the attempted assassination of NATO allied political and military leaders.
- **The drone will always get through:** For the first time in a generation, a viable and deadly threat from hostile enemy airpower has emerged. Advances in range, payload, information transmission, multi-drone teaming and precision-strike necessitate a rethinking of so-called 'Asymmetric Warfare' and existing form of force deployment.
- **Drones can be both unarmed and dangerous:** Unarmed fixed-wing and quadcopter drones, of various sizes, provide state and non-state adversaries with a range of threatening capabilities. For example, at a tactical level, these smaller drones feature prominently in intelligence, surveillance, electronic warfare measures and target acquisition to increase precision lethality from ground-based systems.
- **Beyond the state/non-state nexus:** Drone supplies have moved beyond the control of the nation state as non-state proxies develop their own local manufacturing bases and commercial supply lines.

2 Drone Defence: The Challenges of Countering Drones

- **The defender's dilemma:** 'The good guys need to be on guard always, the bad ones need only to succeed once.' Drone countermeasures should always focus on capturing the human operator and weakening the industrial base, not just stopping the drone.
- **Air defence has been neglected for a generation:** To preserve the tactical and strategical advantage, NATO Members and Partners need to invest in next-generation recruitment, training, and technology for Command and Control and Air Defence.
- **Detection and interception in urban environments:** Drone use in urban spaces opens a vulnerability gap that needs to be taken seriously. A well-defined legal and regulatory architecture matters for both safety and security reasons.

3 Future Threats and Opportunities out to 2035

- **Drone swarms, autonomy, Artificial Intelligence (AI):** Technological advances will allow for a lethal use of unmanned platforms with a decreasing human involvement. This will pose new challenges to drone defences in both qualitative and quantitative terms.
- **Proliferation of land, air, sea, and under water drones will expand the domains and dimensions of drone threats:** 'The Third Drone Age' will be defined by full spectrum drone warfare; a phenomenon that will alter the character of warfare and is thus in need of further evaluation.

Statement of Method and Structure

Jointly led by the Center for War Studies (CWS, Denmark) and the Center for Security Studies (CSS, Switzerland), the *Vulnerabilities of the Drone Age* project ran across 2020 and 2021, taking the form of three virtual Strategic Foresight Analysis workshops. The workshops were closed, encrypted, and held under Chatham House Rules to ensure the delegates could speak freely and openly about the challenges faced. The project's main goal was to bring together experts from across the academic, technological, policy, and military communities to provide NATO Members and Partners with strategic-level, tailor-made insights into what the Alliance should consider while conducting doctrinal development on the problems of drone threats and countering drones across DOTMLPFI. Each workshop lasted approx. three hours and was structured around two sessions. Each session started with a 15-minute opening 'lightening talk' to introduce the topic, set the scene, and inspire debate. The follow-up expert group discussion then elaborated further on the topic through exchanging recent scientific evidence and practical experience for 45 minutes. The first workshop 'Proliferation in the Second Drone Age: The threat of state and non-state drone diffusion' discussed drone technology as a threat due to the malign use of drones by both state and non-state actors. The second workshop 'Countering Hostile Drones: Emerging and Established Capabilities' assessed the current state of counter drone technologies and divulged best practice on effective drone defences, derived from recent experience and the ever-evolving threats posed by hostile actors. The third workshop, 'Foresight Scanning 2035: What's Next for the Drone Age?', forecast what the Third Drone Age might look like out to 2035 based on our current understanding of emerging trends in multi-domain full spectrum drone warfare. This report follows a similar structure, focusing on three sections, 'Drone Attack', 'Drone Defence', and 'Future Threats'.

Overall, the findings published in this report are predominantly based on these three workshops, alongside the organisers' own extensive fieldwork, previous interviews, and 10+ years' experience of tracking global developments in drone warfare.

The authors would like to thank the NATO SPS Programme for funding this activity, the two VDA Project Assistants (Troels and Julie) for their time and dedication, and all those who contributed to the three workshops. All quotes used from the workshops have been anonymised in line with our privacy obligations and guarantees. A designator of 'academic', 'policy, or 'military' will be used alongside key arguments or quotations to ensure a level of transparency and source of knowledge where possible.

1 Drone Attack

The Threat from Hostile State and Non-state Drones.

On January 3rd, 2020, President Donald Trump ordered a lethal drone strike on Iranian military leader Qasem Soleimani, killing him and nine others. On January 3rd, 2022, two armed drones inscribed with the words 'Soleimani's revenge' were shot down as they targeted US troops based at Baghdad airport in Iraq; a clear sign that two years on, the reverberations of Soleimani's assassination are still being felt across the Middle East. Indeed, since 2020, a lot has changed in terms of our understanding and lived experience of both state and non-state drone warfare (Grieco and Hutto 2021). Once the sole domain of select Western and allied nations – such as the United States, United Kingdom, France, and Israel – drones of varying classifications and capabilities have now proliferated across the globe to over 102 different state actors and at least 53 non-state actors (Rogers 2021, Gettinger 2020, Chavez & Swed 2021). Soleimani was killed partly due to his role in supplying Iranian military drones to an array of terroristic proxies who align to Iran's interests. On January 17th, 2022, for instance, Iran-backed Houthi rebels fired drones and missiles at key transport and industrial sites in Abu Dhabi. These lethal attacks killed three people at industrial sites in the city and damaged a new extension of the city's international airport. These strikes marked the start of a week of drone and missile strikes on both US military sites and key strategic targets within the UAE and Iraq. Such attacks are the 'new normal' in terms of threats faced by NATO Members, Partners, and their allies and act as a pertinent reminder of the technological advances made by hostile state and non-state actors in recent years. The NATO SPS funded *Vulnerabilities of the Drone Age* workshops provided a forum within which emerging threats that preceded these latest events could be discussed, analysed, and processed.

Key threats from state and non-state drone attacks:

- **First is the practice of assassination.** In a short period of time, state and non-state actors that had previously been grounded due to a lack of finance, training, or accessibility to high-end military hardware, have gained crude airpower and in many cases their modus operandi mimics tried and tested tactics of drone deployment – assassinations being one (Academic, VDA 1). The targeted use of a radioactive drone against former Japanese PM Shinzo Abe's offices in Tokyo in 2015; the 2018 attempted drone assassination of Venezuelan President Nicolás Maduro; the 2021 drone assassination attempt on Iraqi PM al-Kadhimi all indicate a continuing threat that will likely grow out to 2035 with ever more precise and longer-range drones, including with use of facial recognition. The overall conclusion from the workshops was that 'we have entered a new age of assassinations' (Academic, VDA 3) where weaponised drones with every greater lethality, payload, and range will be increasingly used in the attempted assassination of NATO allied political and military leaders (Military, VDA 3; Callamard 2020, Chávez & Swed 2021).

- **Second is the use of lethal swarming tactics and multi-drone deployments.** No longer used in ones or twos, drones are, and will increasingly be, used in rudimentary swarms out to 2035. This is not to say that 'true swarms – in which small or large drones are able to communicate, interact, and respond in an autonomous manner' will be available to small state and non-state actors by 2035 (Academic, VDA 3). Instead, drones will be deployed in ever greater multiples of 10s, 20s, or potentially 100s as they are sent as part of 'multi-drone and missile launches' towards military, industrial, or civil targets in an attempt to saturate and overwhelm available air defence systems. This was termed 'a swarming tactic' (Academic, VDA 2) and was evidenced by the recent Houthi attacks on the capital city of the UAE, Abu Dhabi, and the frequent attacks on Israel in 2021. *Operation Guardian of the Walls,* in which more than 4,300 rockets and drones were fired towards Tel Aviv and central and southern Israel, demonstrated that even the world's most advanced Iron Dome air defence system was – at points – overwhelmed and a proportion of the strikes broke through existing defences (Academic, VDA 2; Mohammed *et.al.* 2021). Although missiles are still the core concern of the Israel Defense Forces, the increasing use of drones in 'swarming tactic' attacks, posed a major worry due to their ability to loiter, adapt, and evade (Military/Policy, VDA 2). It is in this context, across the land, sea, and air domain, that 'the small and numerous drones will pose a challenge to the big but few Western defence assets' in the region (Academic/Policy, VDA 3). The conclusion from the workshops was that 'the drone will always get through' (Academic, VDA 3; Rogers 2019, Kallenborn 2020).

- **Third is the use of "unarmed and dangerous" drones.** Unarmed drones – both fixed-wing and quadcopter systems – are now a vital part of the precision-strike matrix. Small, inexpensive fixed-wing and quadcopter drones can increase the accuracy, range, and lethality of strikes by artillery, mortars, and missiles. For example, small, fixed wing systems, such as the Russian Orlan-10, have been deployed in all recent Russian con-

flicts (from Syria to Ukraine) and can be used for target acquisition, helping artillery to deliver precision strikes on enemy positions (Rogers & Holland-Michel 2020, Holland-Michel 2020). There are also non-kinetic threats posed by such drones. The Orlan-10s, used in a 'three drone partnership' as a team of systems, can work together to provide near real-time video relay, electronic warfare capabilities, and jamming when attached with a Leer-3 payload (Policy, VDA 2). Non-state actors, such as ISIS, have also utilised unarmed drones to loiter, to provide persistent overwatch, and to pester Western forces during Operation Inherent Resolve (Academic, VDA 1). They have also been used for surveillance and target acquisition, helping to guide sniper fire, vehicle-borne IEDs, suicide bombers, and coordinate ground-based attacks (Military, VDA 1). These tactics of drone use are especially successful in the sheltering volumes of Urban environments or in congested airspaces where similar looking state deployed systems provide an element of disguise and deniability. Unarmed state MALE drones can also be used to help direct and provide intel to proxies from high-altitude and distance, without crossing the threshold of active engagement (Military, VDA 3).

- **Fourth is the blurring of the state/non-state supply nexus.** A key question that arose from the VDA workshops was 'how are drones supplied and manufactured by non-state actors?'. As is often the case when studying the supply of terroristic actors, allied nation states are vital sources of material and training. Iran, for example, has reportedly been supplying a selection of non-state groups across the Middle East that do bidding on Iran's behalf and act as a thorn in the side of the West and its allies. Nevertheless, even when these state-sponsored supply lines are cut off (such as in the case of Iran's supply to Houthi militants), the non-state actors are able to manufacture their own locally produced systems (Academic, VDA 1). By taking fibreglass shells of military grade systems and augmenting them with readily available commercial drone technologies (motors, cameras, transmitters, wiring etc), the non-state groups are able to create a hybrid of state designed drones, powered by commercial systems (Rogers 2021, CAR 2020). This offers the non-state actor the ability to operate autonomous of state supply, to provide their locally produced drones and designs to other non-state actors, and to operate outside of the control or political direction of the original supplying state. The consequences of this are unchecked and uncontrolled drone proliferation by and to non-state actors. This can also lead to further confusion over attribution and deniability as almost identical state designed drones are operated by a wide array of actors across a set geographical space.

Overall, section one of the VDA final report highlights that we have entered a new age of assassinations where airborne drones present a growing threat to allied political and military leaders. At a broader strategic level, it was concluded that due to advances in range, payload, information transmission, multi-drone teaming and precision strike the drone will always get through and will continue to threaten the bases, diplomatic sites and allies of NATO Members and Partners. The issue of supply and demand was also raised, with both state supply and local manufacture noted as the main sources of non-state drone technologies. In terms of emerging technologies, a warning was present about the hostile use of unarmed drones. Described as unarmed and dangerous, they can be used to increase the precision of artillery, while also being used for electronic warfare measures and surveillance. Other technological concerns were raised in the workshops in terms of land, air, sea, and underwater drones which can be used in concert to present a novel, multi-layered threat, but could also potentially be harnessed by NATO Members and Partners. These will be discussed further in section two and three.

2 Drone Defence

The Challenges of Countering Drones.

Unmanned aerial platforms are getting faster, cheaper, and increasingly weaponized. The offensive use of drone capability is not limited to lethal attacks causing casualties, but also includes efforts to inflict material damage and to create psychological effects. Drones can demoralize troops on the ground and, as a propaganda tool, influence public opinion and spread fear among civilians (Archambault and Veilleux-Lepage 2020). From 'do-it-yourself' (DIY) platforms of lower technological sophistication to military grade systems, drones can thus have a large symbolic appeal that can overshadow their limited tactical value. The commercial origin of these drones already makes it difficult to prevent their spread and malign use due to the lack of designation and tracking of these widely available systems. As controlling the proliferation of commercial drones that can be repurposed for combat remains problematic, more policy attention needs to be paid to drone countermeasures in both technical and strategic terms.

Key challenges of countering drones:

- **First is the defender's dilemma.** Hostile actors can use the same cheap commercial drone for different missions (ISR, armed attacks). These multipurpose, malleable commercial drones introduce ambiguity, which makes it difficult to anticipate the parameters of the threat these drones can pose (Academic, VDA 3). DIY drones create unpredictability which complicates the planning of drone defences. Since the technological innovation has moved from defence and security industries to the commercial sphere, especially non-state actors have been more flexible at weaponizing drones than Western nations. This is mainly due to domestic safety and regulatory measures (Academic, VDA 3). As a result, national countermeasures tend to lag this rapid hostile adaptability.

  In addition, it is not only hard to distinguish between birds and quadcopter drones, but it is getting harder to differentiate between drones, other electromagnetic noise, and objects with a similar physical signature; for instance, air-conditioning systems (Academic, VDA 2). Air defence systems designed to deal with manned aircraft or larger missiles have a hard time spotting a small, slow, low flying drone (Academic, VDA 1). Improvements in object recognition and distinction would significantly advance counter-drone efforts.

  Although drones are uncrewed platforms, they are (still) operated by a human (in the first instance at least). Ideally, NATO Members and Partners need to stop attacks before they are in motion. This will require investigative police work and intelligence to identify the operator and the sponsor of drone attacks. Looking more into the spread of commercial drone technology and tactics, techniques, and procedures among criminal actors can help NATO Members and Partners better understand possible future threats, especially in terms of distraction, disruption, and destruction. One such area of interest includes smuggling of contraband past tight security facilities (Policy, VDA 2; Bunker and Sullivan 2021), which can, for instance, inspire hostile actors in their use of drones to attack the bases of allied troops.

- **Second is a generation-long neglect of air defence.** Because drones consist of several components, defence systems have several options in terms of entry points to disable and/or destroy the drone: vehicle itself, its payload, control element (remote control, ground control station, mission control element, external and internal hardware, software), data links (ground air, space segments), human element (launch agent, mission control element, individual drone operator) and support element (Military, VDA 2; Willis *et al.* 2021). This is reflected in the variety of possible countermeasures, which can include kinetic interceptors (missiles, drones, projectiles) and non-kinetic means (lasers, jamming, nets).

  Following the assumption that it is sufficient (and easier) to disable a drone than to destroy it physically, most current military counter-drone systems rely on electronic warfare capabilities to disrupt the communication link between drones and their operators. However, these may no longer be able to stop drones with increasing levels of autonomy. In addition to interfering with air navigation signals and radio transmissions, jamming may become difficult also because the defender has no indication as to the frequency band the hostile home-made commercial drone is using (Academic, VDA 3). Drone defence is further complicated by the fact commercial drones are no longer small, low, and slow, but also include fast racing-grade drones on an automated path. Ignoring these developments can render the newest generation of CUAV systems obsolete even before deployment and delay the development of useful defensive systems.

  As to swarms, it may be tempting to discount what the specific definition of swarms is decided upon as a matter of semantics, since the effect is perceived to be the same no matter the technical sophistication, that is large numbers overpower defence

capabilities. From a countermeasure point of view, however, autonomous swarms can 'counter the countermeasures' in ways that swarms simply flying in rudimentary formation are not capable. Autonomous swarms act differently towards loss. Unless the countermeasure is strong enough to engage the whole swarm at once, true swarms, driven by real-time machine learning, would react in a more dynamic, unpredictable, and adaptive way than 'dumb' systems used in a swarming tactic (Military, VDA 3).

Multi-layered air defences will become indispensable for an effective defence against drones of all shapes and sizes. This implies that to counter the drone threat, training of anti-aircraft artillery units needs to be adapted as well to reflect the technological advancements. For instance, camouflage does not work against LIDAR sensors, which are today found even in iPhones (Willis *et al.* 2021). Furthermore, with the advent of swarms, AI-enhanced drone countermeasures, specialistic training, tailored recruitment, and simulation will become necessary to keep pace with indeterministic and collaborative drone attacks (Military/ Academic, VDA 3).

- **Third is detection and interception in urban environments.** The drone threat from the sky in an urban space opens another vulnerability gap that needs to be taken seriously. However, the expert community disagrees about how significant the domestic urban drone threat will become by 2035. Some observers warn against the risk of exaggerating the effects of a malign drone use (Military, VDA 2). Since drones are versatile platforms, from flying into buildings to identifying people, it is not surprising that a lack of understanding within policy-making circles can lead to blown-up expectations as to both the gravity of the threat and the requirements of effective defence measures. Better analyses of how drones change and challenge urban airspaces will help to correct these misperceptions (Policy, VDA 3) and inform the debates on whether the drone threat justifies investments of scarce resources into measures that specifically counter drones.

  At the national level, drone proliferation is approached in two different ways: safety and security. This means that governments are funding not only measures to mitigate drone expansion risks (unmanned traffic management) but also countering systems. Drone traffic will increase in civilian airspace, requiring new operational and safety regulatory measures. It will also introduce problems with bandwidth availability and new environmental risks (noise and visual pollution). For instance, the European Commission's U-Space and its handbook on countering drones both aim to improve air traffic safety and prepare cities for dealing with non-cooperative drones (European Commission 2022). Importantly, drones will not only become a threat to critical national infrastructure, but also vital national infrastructure themselves, as in logistics and transportation services (Academic, VDA 2; Rogers 2019).

  Drone threats are not only a military problem. The non-battlefield use of drones in the urban environment can include providing a view from above for spying on critical infrastructure (police stations, military installations, nuclear powerplants), carrying capacity (smuggling, drug-trafficking), disrupting law enforcement (as well as political or sport events), and weaponizing drones to inflict harm and to distribute harmful materials (radioactive sand, hazardous biological/chemical agents) (Academic, VDA 2). The form in which these drones are deployed is characterized by their innovative morphology, autonomy, and DIY practices (Jackman 2021).

  A well-defined legal architecture matters in domestic urban spaces for both safety and security reasons. Defining the area of responsibility usually gets political regarding which authority should be in charge. Disagreements over drone responsibility can lead to delayed implementation. Homeland security and law enforcement agencies usually act as the first responders, working across both safety and security. However, even if national authorities are more aware of what happens within the drone space, the spectrum is still very complicated and many countering systems are not working perfectly. New performance and safety standards of interdiction technologies are expected in the civilian environment. For instance, reducing the risk of rogue operations through built-in geofencing capabilities—to prevent the drone from entering airspace that is off-limits to drones—is challenging as it requires keeping the data on airspace up to date and remote identification for all drones, including recreational ones.

  Given the variety of attacks provided by the malleability of drones entering airspace, some national policy makers question whether it is politically justifiable and proportionate to expand defence structures to counter civilian drones. The adoption of all technologies comes with a societal risk that must be lived with. However, existing defence tools might be more capable to intercept military-grade platforms than commercial drones due to pre-existing threats and precedents (Academic, VDA 2). Small drones have begun to pose a widening and complex threat and still await political appreciation (Academic, VDA 2).

3 Future Threats and Opportunities out to 2035

The VDA report concludes with a selection of the future threats and areas for future research. While Sections One and Two include established and some projected threats, this Section details threats and opportunities out to 2035:

- **Proliferation of drone technology and AI-driven drones.** Technological advances will allow for a lethal use of unmanned platforms with a decreasing human involvement that will pose new challenges to drone defences in both qualitative and quantitative terms. Qualitative, because drone threats are likely to increase in conjunction with other emerging technologies (autonomy, AI, materials). Although drones are currently relatively unintelligent systems with little self-defences, greater risks are to come as the performance of small drones is likely to be improved by the advancements in AI (Academic, VDA 2). AI already plays a central role in increasing autonomy of unmanned systems through machine learning and big data. Greater degrees of autonomy will improve functionality of drones that will enable greater precision of observation and air strikes. Yet, AI-driven drones are only as good as the algorithms they work with and the data they are fed on, so their added value will likely remain limited to the tactical level in the short term.

  Quantitative, because the number of hostile drone operators and the number of drones used in a single attack increase. The global 'dronescape' continues to be shaped by state and non-state newcomers. Although the United States, United Kingdom, France, and Israel have traditionally been the main actors on the global market of large drones (Kunertova 2021a), China, Iran, and Turkey have already changed the texture of drone proliferation, with China becoming the world's number one exporter of armed drones (Wezeman et al. 2019, p. 10). At the other end of the proliferation fork, the shift from cost-prohibitive, inaccessible, and technically complex military technologies to cheap and simple civilian platforms will accelerate. Drones will continue to spread to non-state actors, providing them with a low-cost capability to conduct surveillance, battlespace management, propaganda, and aerial strikes.

- **Looking to 'The Third Drone Age'.** In VDA Workshop 3, a robust discussion about the vulnerabilities of the Drone Age out to 2035 led to some disagreement on the future character of warfare, but also to some points of consensus. It was agreed that by 2035 any discussion about 'A Third Drone Age' would involve an analysis of Uncrewed Underwater Vehicles (UUVs), Uncrewed Surface Vehicles (USVs), Uncrewed Ariel Vehicles (UAVs), and Uncrewed Ground Vehicles (UGVs). By this time, it is expected that hostile state actors will be experienced in the manufacturing, deployment, and supply of these systems to non-state proxies. The terms 'full spectrum drone threats' and 'full spectrum drone warfare' were utilised in the workshop to epitomise the multi-layered and multi-domain character of the threat (Academic/Military, VDA 3).

  Although further exploration of 'The Third Drone Age' and 'Full Spectrum Drone Warfare' is required, the growing presence of automated multi-drone deployments and autonomous/AI drone swarms in the air, on land, and at sea was expressed as both an emerging challenge and potential opportunity for NATO Members and Partners to build up their own capability gaps, such as in border patrol or uncrewed submarines (Kunertova 2021b). Such matters require further research to expand our understanding of the future threat landscape. It was concluded that FICINT (Fictional Intelligence, also known as Useful Fiction) would be a useful method to facilitate this research.

  Looking ahead over a decade and deciding which state and which non-state actor will be threat does not just pose a problem in predicting the rapidly changing geopolitical landscape, but also tactics given the pace of evolving technology. Ultimately, technology will provide means, but not without budgets and policy. NATO Members and Partners will need to rethink where to cut 'sacred cows' vulnerable to drones and rethink recruitment and expertise for drone and countering drones (Singer and Cole 2015). They need to strike the right balance to avoid overhyping the drone threat and underestimating the malleability of commercial and military drone technologies.

References

Archambault, E. and Veilleux-Lepage, Y. (2020). 'Drone imagery in Islamic State propaganda: flying like a state', *International Affairs* 96 (4): 955–973.

Bunker, R. J. and John P. Sullivan, J. P., eds. (2021). *Criminal Drone Evolution: Cartel Weaponization of Aerial IEDs,* Bloomington: Xlibris, 2021.

Callamard, A. (2020). 'Report of the UN Special Rapporteur on extrajudicial, summary or arbitrary executions to the Human Rights Council Forty-fourth session', A/HRC/44/38.

CAR, (2020). 'Iranian Technology Transfer to Yemen', *Conflict Armament Research.*

Chávez, K. and Swed, O. (2021). 'The proliferation of drones to violent nonstate actors', *Defence Studies* 21(1): 1–24.

European Commission (2022). 'Unmanned Aircraft', DG Defence Industry and Space.

Grieco, K. A. and Hutto, J. W. (2021). 'Can drones coerce? The effects of remote aerial coercion in counterterrorism', *International Politics.* [published online]

Holland-Michel, A. (2020). Unarmed and Dangerous, The Center for the Study of the Drones, Bard.

Jackman, A. (2021). 'Visualizations of the small military drone: normalization through "naturalization"', Critical Military Studies.

Kallenborn, Z. (2020). Swarms of Mass Destruction: The Case-for Declaring Armed Fully Autonomous Drone Swarms WMDs, Modern War Institute: West Point.

Kunertova, D. (2021a). European Drone Clubs Stall Strategic Autonomy, Center for Security Studies, *CSS Policy Perspective* 9 (5).

Kunertova, D. (2021b). From Robots to Warbots: Reality Meets Science Fiction, Center for Security Studies, *CSS Analyses in Security Policy* no. 292.

Mohammed, A. *et.al.* (2021). Israel's Gaza challenge: stopping metal tubes turning into rockets, *Reuters.*

Rogers, J. (2019). The Darkside of Our Drone Future, *The Bulletin of the Atomic Scientists.*

Rogers, J. (2020). Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age, NATO JAPCC.

Rogers, J. (2021). 'Last month, three drones attacked an Israeli tanker. Here's why that's something new', *The Washington Post.*

Rogers, J. and Holland -Michel, A. (2020). 'Drone Warfare: Distant Targets and Remote Killings'. In Thapa, M., Marton, P. and Romaniuk, S. N., eds., *The Palgrave Encyclopaedia of Global Security Studies.* London: Palgrave.

Singer, P. and Cole, A. (2015). Ghost Fleet: A Novel of the Next World War. New York: HMH

Wezeman, P. D. et al. (2019). Trends in International Arms Transfers 2018, Stockholm International Peace Research Institute.

Willis, M., Haider, A., Teletin, D. C. and Wagner, D., eds. (2021). A Comprehensive Approach to Countering Unmanned Aircraft Systems, NATO: The Joint Air Power Competence Centre, 2021.

About the Authors

CENTER FOR WAR STUDIES

Dr James Rogers is DIAS Associate Professor in War Studies, within the Centre for War Studies, at SDU,and Associate Fellow within LSEIDEAS, at the London School ofEconomics. He is currently an Expert Advisor to the UK Parliaments All-Party Parliamentary Group on Drones and Modern Conflict, a UK MoD Defence Opinion Leader,and the NATO Country Director of the Vulnerabilities of the Drone Age project, supported by NATOSPS. He has previously been a fellow at Stanford University, Yale University, and the University of Oxford and currently heads BISA War Studies, the War Studies section of the British International Studies Association. James is also a Non-Resident Senior Fellow of the Cornell Tech Policy Lab at Cornell University.

CSS ETH Zürich

Dr Dominika Kunertova works as Senior Researcher at the Center for Security Studies at ETH Zurich. She researches trends in military technology, geopolitics of emerging and disruptive technologies, and transatlantic defence and security cooperation. She is also NATO Partner Country Director of the Vulnerabilities of the Drone Age project, funded by NATO SPS. Her previous work experience includes strategic foresight at NATO Allied Command Transformation in Norfolk, capability development at NATO Headquarters in Brussels, and military unmanned systems at the Center for War Studies in Denmark. She holds a PhD in Political Science from Université de Montréal and has published articles and research reports on NATO burden-sharing, military drones, and missile technology.

NATO OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme