



A pilot from 408 Tactical Helicopter Squadron does the last of his pre-flight checks before taking flight in a CH-146 Griffon helicopter, near the training area of Wainwright, Alberta during Exercise INTREPID BEAR 22 on May 4, 2022.

Photo: Master Sailor Dan Bard, Canadian Forces Combat Camera, Canadian Armed Forces photo

Cybersecurity and Air Power: Keeping Humans in the Loop

KRISTEN CSENKEY AND ALEXIS RAPIN

Dr. Kristen Csenkey is a Social Sciences and Humanities Research Council (SSHRC) postdoctoral fellow at the Brian Mulroney Institute of Government, St. Francis Xavier University. She is also a fellow with the Canadian Maritime Security Network, the Centre for Military, Security and Strategic Studies at the University of Calgary, and the North American and Arctic Defence and Security Network (NAADSN), among others. Dr. Csenkey has previously led multiple Department of National Defence-funded projects on the defence and security implications of quantum technologies, connected aviation systems, and cyber-resilient electric vehicles. She currently leads a SSHRC Partnership Engage Grant focused on responsible global quantum technology governance. She holds H.B.Sc., M.A., M.A.P., and Ph.D. degrees.

Alexis Rapin is an associate fellow with the Raoul-Dandurand Chair of Strategic and Diplomatic Studies (affiliated with the University of Quebec in Montreal). His research focuses on cybersecurity and on the international security implications of digital technologies. In 2023, he testified before the Standing Committee on National Defence of the House of Commons of Canada on issues related to Canadian cyber defence and strategy. He is also a member of the editorial committee for Le Rubicon, a francophone platform dedicated to the analysis of international and strategic affairs.

In their novel *2034* (published in 2021), authors Elliot Ackerman and former United States (US) Admiral James G. Stavridis imagine a major future conflict between the United States and China.¹ The first pages open with an incident in which an American F-35 fighter is suddenly captured by Iran, after a cyber attack has enabled them to remotely take control of the aircraft. Later in the book, faced with a desperate situation, the US Navy decides to retire its F-35 fleet and reactivate its old F-18s, which are stripped of most of their on-board electronics in the process. As its adversaries have managed to compromise its high-tech aircraft, the United States is forced to rely on its technological ancestors, assumed to be digitally safer.

Although an intriguing and fictional situation,² the scenario narrated in *2034* relates to an idea gaining traction in the strategic literature: namely, that the current approaches to technological superiority that have been the hallmark of Western militaries for almost 40 years may now represent a vulnerability.³ As cyber-warfare capabilities expand, it now seems possible for adversaries to take advantage of the emerging dependencies and possible vulnerabilities associated with highly connected technologies. Additionally, varying collective risk management practices, as well as legacy systems and an enlarged attack surface, increase exposure to sophisticated cyber attacks and potentially compromisable electronic components, systems, processes, technologies and people. We can observe this blending and complexity materializing in current geopolitical conflicts. For example, in the face of the ongoing Russian invasion, the Ukrainian military is reusing old field telephones along the frontline, fearing that its modern transmission systems may be compromised by its adversary.⁴

In this paper, we take an expansive view of cyber-warfare and connected technologies, encompassing both cyber and electronic warfare. Although operations in the cyber domain and electromagnetic sphere can have distinct characteristics (especially with regard to the units, capabilities and know-how involved), we focus on the implications of the associated human and technological vulnerabilities, capabilities and activities. Broadly, we contextualize this situation as part of a holistic cyber concept where electromagnetic tools, such as radio frequency jamming, and cyber tactics, such as hacking, comprise a dynamic space where humans and technologies interact in a digital-physical environment.⁵ This environment poses challenges for operations and activities in all domains, and we thus argue for solutions to both human and technical vulnerabilities.

The problem of interconnected technologies and threats proves especially meaningful to the aviation sector, in which aircraft, drones, helicopters,⁶ and the digital-physical infrastructure that supports them are now highly digitized and connected. In a scenario that may well have inspired Ackerman and Stavridis, in 2011, the United States lost an observation drone after Iran hacked into its GPS system to land the drone on an Iranian base.⁷ Drones are no longer considered part of a “poor man’s air force,”⁸ especially when paired with new cyber tactics,⁹ procedures,¹⁰ and increasingly available commercial technologies.¹¹ Others have also detailed how the F-35, which is deployed by a

growing number of Western armies, represents the epitome of a weapon system that is highly vulnerable to cyber threats.¹² Cyber threats are no longer a hypothetical danger: they are a reality for modern air forces to constantly be aware of, act upon, mitigate, and understand in terms of their connections in digital-physical spaces. The challenge before the forces is clear: identify how to deal with these threats, without renouncing their cutting-edge technologies.

“Cyber threats are no longer a hypothetical danger: they are a reality for modern air forces.”

One of the major issues is that the military “techno-solutionism,” inherited from the 1990-2000s,¹³ may be replaced by a “techno-pessimism,” in which armed forces in general (and air forces in particular) may have declining confidence in their high technologies and devices and end up discarding some of them, as in *2034*. Indeed, one of the great strengths of cyber capabilities is not only that they may undermine the availability and usability of military technologies, but also that they reduce the trust placed in them by a decision maker. By simply instilling doubt about the integrity of a system, cyber attacks may dissuade an actor from using a wider set of capabilities, thus producing a result disproportionate to their actual effects. Some, such as Christopher Coker,¹⁴ have surmised that this could be the future strategy of foreign powers like China. A state could attempt not to match a technologically superior competitor, but instead force a reduction in the use of certain technologies by persuading the adversary that these have been compromised or rendered inept.

Consequently, cultivating and securing the confidence of Western militaries in the technologies they employ, and in which they have invested considerable resources, appears to be a crucial issue of strategic importance.¹⁵ This may prove all the more important in a crisis context, where quick and difficult decisions may have to be made about the reliability of information technologies. The aim of this article is to present possible solutions to this challenge. We propose an approach that puts people at the heart of securing air power against cyber threats. This involves

cultivating the human capital and organizational structures needed to maintain a high degree of trust and technological resilience within an air force. As the Royal Canadian Air Force celebrates its centennial, adapts to defend and protect Canada, and continues to support the defence of North America with the United States, there is an opportunity to explore the increasing connectivity between domains, technologies, and the continued importance of people in a dynamic environment.

Boyd 2.0: Reinventing the Loop

To fully understand the issue at hand, we must first go back to the origins of the techno-solutionist paradigm and especially to one of its key concepts: the famous “OODA loop” (for Observe, Orient, Decide, Act), theorized by US Air Force Colonel John Boyd in the 1980s.¹⁶ Intended to describe the process by which an actor perceives a situation, analyzes it, deliberates, and acts accordingly, the OODA loop has since acquired much celebrity and—for better or worse—has been applied to a variety of non-military purposes, from business to sport. In the military domain, the OODA loop concept gradually gave rise to a full-fledged theory of victory, embraced by several major Western armed forces,¹⁷ such as the United States, the United Kingdom and France.¹⁸ In short, the core concept is that an actor who manages to complete the OODA cycle in the shortest possible time acquires an advantage over their adversary. Among other advantages, a rapid completion of the OODA loop is assumed to provide an actor with better situational awareness, ultimately enabling them to control the tempo of operations.¹⁹ Over the course of the 1990s, this logic led militaries to acquire increasingly sophisticated Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) technologies, to rapidly complete the OODA loop.

The OODA loop paradigm may now appear undermined by the increasing complexity and development of electronic and cyber-warfare capabilities. As cyber means have the potential to compromise the information technologies upon which the fluidity of the OODA loop heavily depends, they seem to threaten the viability of a way of war largely based on technological and information superiority.²⁰ Some approaches to contextualizing cyber operations demonstrate that an adversary can be restrained in the context of open warfare by hacking their information collection capabilities or communications systems.²¹ In this regard, cyber threats appear of particular importance in the air domain, where digital technologies are not only omnipresent and critical to mission completion, but also represent potential attack vectors. Indeed, air forces around the world must now contend with cyber-related threats, the risks enmeshed within the usage of and connection to complex technologies, and varying human actions, such as GPS spoofing,²² onboard software hacking,²³ or compromised data links,²⁴ in addition to threats relating to ground bases and physical installations. For instance, during the 2019 Gulf of

Oman crisis, the US military hacked a database operated by the Islamic Revolutionary Guards in order to cripple Iran’s targeting capabilities (including through the use of attack drones).²⁵ The above-mentioned vulnerabilities, if exploited, may considerably slow down or even paralyze the completion of the OODA loop.

In spite of its many uses and misuses throughout the years, the OODA loop remains a useful thinking framework for our purpose, as it helps emphasize two crucial aspects related to the management of cyber threats. First, the principle of the OODA loop is applicable to situations relating to cyber attacks, posture and planning. When faced with a cyber incident, for example, a military must ultimately be able to *Observe* the impact of hacking activities, *Orient* itself amidst the impacts caused by the attack, *Decide* with confidence which capabilities are compromised and which remain serviceable, and finally *Act* on the basis of this analysis. The OODA loop concept can thus be applied to understanding the impact of an attack and the appropriate resulting actions. To be sure, the OODA loop is not used for reacting to a cyber incident; however, it is a useful concept to develop confidence in both people and technologies, as we will further demonstrate.²⁶

Second, although information technologies appear to be important enablers and accelerators of the OODA loop, they are by no means its only components. The processes by which a military gathers and processes information include crucial human and organizational components, which are as important as the technologies themselves.²⁷ As others have shown, modern militaries may display a less-than-optimal use of cutting-edge technologies due to poor management of human and organizational issues.²⁸ Of course, an increase in the speed of completion of the OODA loop is not the only factor in achieving mission success in modern warfare. Nevertheless, human and organizational components are involved in the process and must be further developed to ensure its rapid completion. The challenge then becomes trying to determine how to make the best use of available human and organizational resources to maintain or re-establish the fluidity of the OODA loop in a context where technologies are (or appear to be) degraded.

In the sections that follow, we provide examples drawn from Canada’s international allies, as well as suggestions to further develop resilience in digital and physical contexts of conflict. We conclude by drawing together our discussion and recommendations in the context of NORAD modernization and cooperation, as emphasized in the recently released defence policy update, *Our North, Strong and Free: A Renewed Vision for Canada’s Defence*. In doing so, we make connections between cyber, air, and people power.

Train and Plan: Preparing for Crisis Scenarios

There are several measures that militaries can take to anticipate and prepare for major cyber attacks. These measures may include conducting exercises that simulate military systems being compromised. As early as 1997, the US Department of Defense (DoD) conducted their first such exercise, *Eligible Receiver 97*, in which a National Security Agency (NSA) red team attempted to infiltrate the US Indo-Pacific Command's networks.²⁹ Although the results proved catastrophic for the defenders, the exercise nevertheless helped identify various areas of cyber vulnerability within the DoD and demonstrated several ways to harden their defences. Such practices have since become increasingly common,³⁰ and take on a variety of forms.

These exercises are frequently practiced on an annual basis, and can include multinational cooperation, bring together mainly cyber specialists, and aim to simulate the active defence of a network against hypothetical hostile actors. Other types of exercises involve "traditional" forces who practice their ability to operate in the context of cyber attacks, with the goal of cultivating a conventional unit's digital resilience. France, for instance, is increasingly conducting such training in "digitally degraded conditions" to better prepare units to carry out a mission even when certain technologies are rendered unavailable or unusable.³¹

Exercises combining digital and traditional approaches can be particularly useful because they bring together cyber specialists and conventional forces personnel, and train units to synchronize their operations with cyber protection and remediation efforts. Several authors define this kind of synergy as "mission assurance," whereby an organization's mission capability is safeguarded by specific processes in the event of a system failure.³² For example, in early 2024, the French Air Force simulated a cyber attack (and the restoration) on a *Phénix* refueling and transport aircraft's onboard system,³³ bringing together aviators and cyber defence personnel as part of the major annual DEFNET exercise.³⁴ In such cases, the aim is not only to train a command to switch back to legacy technologies (in the manner of 2034), but also to practice confidently identifying the systems that remain trustworthy and those that seem compromised, and assessing the viability and speed of their restoration to operational status.³⁵ In other words, such exercises create opportunities to simulate and train in the *Observe* and *Orient* phases of the OODA loop in the context of cyber attacks.

Additionally, these types of exercises can help a military develop another important tool of resilience: contingency plans. Pre-established procedures can stipulate the appropriate actions in a crisis scenario where technological capabilities are degraded. In the air domain, the US Air Force is currently testing navigation methods based on the analysis of anomalies in the earth's magnetic field to help its pilots find their way even if their GPS is neutralized.³⁶ These are only a few examples of procedures that

“ Like a jigsaw puzzle, the coherence of a military organization depends not only on the presence of all the pieces, but also on their appropriate position within the ensemble.”

can be devised and deployed in the event of a cyber attack. These types of responses, however, should be a part of comprehensive contingency plans, including ensuring that personnel have a minimum level of training in using alternative or "low tech" methods. When properly designed and disseminated, such plans can facilitate the *Decide* and *Act* phases of the OODA loop. These plans can serve to provide tested and potentially viable options for commanders and ensure that tasked personnel have the necessary information for implementation.

Organize: Keeping Your Friends Close

Another set of measures that can increase an air force's resiliency to cyber threats relates to its organizational and bureaucratic structure: specifically, to the place occupied by cyber defence personnel within that structure. Like a jigsaw puzzle, the coherence of a military organization depends not only on the presence of all the pieces, but also on their appropriate position within the ensemble. The challenge in this case is to ensure that the "cyber pieces" of an air force are arranged in such a way as to be able to react effectively and efficiently in the event of a crisis.

As in many organizations, a major challenge lies in the fact that cyber defence specialists and units often remain a peripheral support element of military organizations, isolated from decision-making centres. Field commanders and cyber defence specialists do not often collaborate and may not really *know* each other professionally. To make matters more complicated, the two groups may have different educational backgrounds and ways of communicating about operational problems, and thus may not *understand* each other. As Michael Hayden, former US Air Force General and later NSA Director, laments: "After a few sentences, the cyber briefer often sounds vaguely like Rain Man to many of the seniors in the room. With a few more sentences, most are convinced that he is."³⁷ Speaking the same language and being able to switch between languages may prove useful in bridging gaps in strategic and operational planning.

This gap is especially problematic because cyber threats can produce major effects on the trust that militaries place in technologies without nuance about the interconnections



Tactical Air Control Party (TACP) personnel coordinates information between the aircrafts and Joint Terminal Attack Controller (JTAC) to make a successful air drop, taken on June 23, 2026 at Primrose lake, Alberta.

Photo: Corporal Connie Valin, Canadian Armed Forces photo

and complexities embedded within digital-physical systems. A component of this trust is based in part on the confidence that “traditional” military personnel place in the cyber specialists tasked with securing their systems.³⁸ To be sure, securing systems is not a function for cyber specialists alone – there is a broader role for commanders and their staff to play. In the military world, as in other contexts, it is easier to trust someone you know, and whose expertise you have already seen and experienced. More meaningful integration and interaction of an air force’s cyber personnel into its overall operations could be an organizational priority to consider, in addition to fostering mutually trusting relationships where commanders understand their dependence on cyberspace. Commanders would need to ensure that they and their staff (including the cyber specialists) play a role in the defence of systems. This cultivation of trust and expertise is especially important as many cyber attacks exploit human and technical vulnerabilities.

For instance, meaningful integration may involve setting up reciprocal learning mechanisms that enable personnel to better understand what cyber specialists do, how they think and work, and how this work fits into the strategic, operational, and organizational functioning of an air force. Other efforts may involve simply bringing cyber specialists physically closer to certain areas of operation. In the current war in Ukraine, for instance,

Ukrainian and Russian forces have reportedly started to position cyber teams closer to the frontline, to better coordinate with forward-deployed troops (this decision may be due in part to the importance of ensuring the effective operation of drones).³⁹ In addition to shortening the communication chain, bringing diverse teams together may help both cyber operators and traditional personnel to better understand each other’s needs and foster greater synergies.⁴⁰ Introducing this proximity or familiarity may thus contribute to streamlining the efficiency of the OODA loop process.

Inspire: Creating the Right Incentives

The isolation of cyber specialists is not only due to their position in the organizational chart, but is also rooted in organizational cultures that influence the way they are viewed by the military community. Whether army, navy or air force, military organizations maintain certain norms, ideas and traditions that they perpetuate over time.⁴¹ These specific cultures have a direct impact on the way organizations work; however, they can also contribute to issues relating to operational posture.

In an article, Rebecca Slayton explores how the persistence of the cult of the “warrior figure” directly contributes to the ostracization of cyber specialists in the US military.⁴² The warrior figure paradigm refers to an institutional reverence for

individuals from certain services, such as special forces or combat arms personnel, whose functions are perceived as more noble because they are closer to the martial ideal of the traditional soldier.⁴³ In the aviation domain, this logic applies particularly to the pilot figure, which is associated with an image of authority largely cultivated in popular culture.⁴⁴ As a result, these positions are often perceived to hold greater credibility in the military establishment to the detriment of branches seen as “less combative” and secondary, such as logistics or communications. There are practical implications of the cult of the warrior figure: for example, functions considered more prestigious are often guaranteed privileged access to certain positions or commands,⁴⁵ potentially making certain career choices more attractive than others.

Cyber specialists, who are not typically perceived as “real warriors,” may be negatively impacted by the perpetuation of the cult of the warrior figure. These negative impacts can include being more confined to menial roles, slowly climbing the institutional hierarchy, and being less likely to obtain certain prestigious commands.⁴⁶ Inevitably, this reality pushes many potential recruits towards other military functions or encourages experienced cyber specialists to join the civilian sector (where there are considerable opportunities in this domain).⁴⁷ In the United States, the US Air Force remains the service whose organizational culture has historically proved most welcoming to cyber specialists, perhaps due to a long standing “victory-through-technology” institutional mindset.⁴⁸ Yet, even in this seemingly successful case, the cyber-warrior status remains largely supplanted by the pilot as the ideal warrior figure. In a 2019 study, the RAND Corporation found that fighter pilots, followed by bomber pilots, remained by far the two most promising career paths for those wishing to climb the US Air Force hierarchy among the US military services.⁴⁹

If an air force aims to effectively deal with cyber threats in the future, then the status of cyber specialists needs to be elevated and paired with greater incentives to encourage members to embrace this vocation. This may involve reforming established recruitment, training, and retention mechanisms, or as Nicholas Romanow terms it, the “Cyber Talent Management Triad.”⁵⁰ Romanow argues that although military leaders understand the importance of cyber operations, there is a shortage of personnel to fill associated roles, and this may be because of workforce competition with the private sector and a military culture that is not attractive to the cyber community. One way to rectify this problem is to invest in developing strong cyber leaders and drawing on the military’s established service culture.⁵¹ The US Air Force recently launched a program aimed at accelerating the commissioning of cyber specialists.⁵² With a view to revising the traditional military career pipeline, one of the aims of this program is to reward cyber-related skills (relative to other conventional military experiences). Another is to make it easier for cyber professionals to attain a rank and pay that is comparable to related positions within the civilian sector.

As authors such as Max Smeets have shown, developing a military’s cyber capabilities requires properly combining a wide range of skills and people—and this goes beyond strictly technical personnel.⁵³ If human capital is important in maintaining the confidence of militaries in their technologies, and if human assets are deemed critical to the effective completion of the OODA loop process, then cyber personnel should feel encouraged and meaningfully engaged in this endeavour. In this case, the training and education of cyber personnel could be expanded to include cyber specialists, leaders and generalists. The bottom line is that all military personnel—particularly those in command positions—need to have the skills to understand their mission dependence on cyberspace and play their role in addressing cyber mission risk.

Conclusion

Maintaining confidence in digital technologies in the face of cyber threats must be paired with confidence in humans and their ability to work together. As we have shown, actively practicing cyber attack scenarios and developing contingency plans to deal with such situations help build and maintain confidence. Another approach is to focus on organizational structures with the aim of better integrating cyber specialists and establishing greater familiarity and synergy with other personnel. Shifts in organizational culture may also play an important role in confidence-building by creating greater incentives for individuals to embrace cyber-related functions.

“ Maintaining confidence in digital technologies in the face of cyber threats must be paired with confidence in humans and their ability to work together.”

In the recent defence policy update, the Department of National Defence details plans for implementing several technological innovations within NORAD, including in the domain of information and communication, stressing the need for command and control “to be digitalized to operate at machine speed.”⁵⁴ In this regard, Canada has begun adopting and integrating cloud-based command and control systems for Canada-based NORAD installations.⁵⁵ Although these new technologies provide opportunities for increased information flow, data collection, and analysis for enhanced situational awareness, they must be considered as a part of a system—or embedded within the loop with humans. Another important aspect to consider is that NORAD is a



Members of the Canadian Fleet Diving Unit (Atlantic) discuss with a member of the French Armed Forces about his explosive ordnance disposal (EOD) tool during the last day of EX NORTHERN CHALLENGE 2024, on October 9, 2024 in Keflavik Iceland.

Photo: Felix Chagnon

partnership based on interoperability and trusted cooperation. As such, confidence in information technologies is important; just as traditional personnel need to trust a cyber operator's capacity to secure their systems, the bi-national partners must promote and maintain trust in their ability to maintain the integrity of their

NORAD-related networks. Paying close attention to the human component of cyber may prove important in rectifying recruitment and retention issues within the Canadian Armed Forces.⁵⁶ Thus, the Canadian Armed Forces in general, and the Royal Canadian Air Force in particular, has a clear interest not only in ensuring that it remains an attractive employer for cyber professionals, but also in making the best possible use of the innovative people power it currently possesses in this domain.

While information technology is both a key component and a source of vulnerability for modern militaries, human and organizational factors represent critical safeguards for guaranteeing their operational capabilities. In this article, we sought to contextualize the problems associated with cyber within the air domain. The issues we raised are relevant for leadership in the Royal Canadian Air Force to consider both individually and jointly with the Canadian Army and Royal Canadian Navy. Long-term cybersecurity planning requires a whole-of-forces approach—not silos. We demonstrated that various instruments already exist, or are in development, and may be leveraged in a meaningful way. As the integration of emerging technologies becomes a priority area in continental defence and in other trusted cooperations,⁵⁷ allies will need to ensure that they are future-proofing technological and human capabilities to defend in unison. Faced with the risk of excessive techno-pessimism, air forces can therefore work towards maintaining confidence in their digital technologies by making sure they “keep humans in the loop.”

Notes

- 1 Elliot Ackerman, and USN Admiral James Stavridis (ret.), *2034: A Novel of the Next World War*. New York, Penguin, 2022.
- 2 For other examples of similar fictional scenarios, see P. W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War*, Houghton Mifflin Harcourt, 2015. For a critical perspective on the use of speculative fiction, see Col. Mark D. Jacobson, “The Uses and Limits of Speculative Fiction: Three Novels about a US-China War,” *Journal of Indo-Pacific Affairs*, August 2023, 1-10.
- 3 See Bruce Schneider and Tara Wheeler, “Hacked drones and busted logistics are the cyber future of warfare,” Brookings Institution, 4 June 2021. Originally found at: <https://www.brookings.edu/articles/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/>
- 4 Jonathan Beale, “Ukraine war: How old tech is helping Ukraine avoid detection,” *BBC World*, 3 May 2023. Originally found at: <https://www.bbc.com/news/world-europe-65458263>
- 5 For a discussion on the distinction and convergence of cyber and electronic warfare, see Ryan J. Worrell, *EW and Cyber Convergence: Beyond Information Warfare*, Air Force Fellows Program, 2020. Originally found at: <https://apps.dtic.mil/sti/pdfs/AD112357.pdf>
- 6 A note on terminology: in an aviation context, both drones and helicopters are examples of aircraft. There are different ways to classify drones based on national doctrine, such as unmanned/uncrewed/
- remotely piloted aircraft systems, and each comes with varying cyber vulnerabilities and characteristics. For more detailed distinctions between drone classification types, see Maj. Osman Aksu et al., *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Joint Air Power Competence Centre, January 2021. Originally found at: <https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf>
- 7 Scott Peterson, Payam Faramarzi, “Iran hijacked US drone, says Iranian engineer,” *Christian Science Monitor*, 15 December 2011. Originally found at: <https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer>
- 8 Nick Waters, “The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria,” *Bellingcat*, 12 January 2018. Originally found at: <https://www.bellingcat.com/news/mena/2018/01/12/the-poor-mans-air-force/>
- 9 Dan Black and Gabby Roncone, “The GRU's Disruptive Playbook,” *Mandiant Blog*, 12 July 2023 [updated: 3 April 2024]. Originally found at: <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>
- 10 Mauro Gilli and Niklas Masuhr, “Drones enhance defences in the Ukraine war,” *Binding Hook*, 10 January 2024. Originally found at: <https://binding-hook.com/articles-hooked-on-trends/drones-enhance-defences-in-the-ukraine-war/>
- 11 See, for example, in Sam Skove, “Army puts drones front and center in unfunded wishlist,” *Defense One*, 22 March 2024; Sam Skove, “Army announces plan to help spread commercial drones across infantry units,” *Defense One*, 27 March 2024; Maxine Baen, “Army tests commercial satellite internet in pilot program,” *U.S. Army*, 28 February 2022. Originally found at: <https://www.defenseone.com/technology/2024/03/army-puts-drones-front-and-center-newly-obtained-budget-docs/395182/>, <https://www.defenseone.com/threats/2024/03/army-announces-plan-help-spread-commercial-drones-across-infantry-units/395260/>, and https://www.army.mil/article/254316/army_tests_commercial_satellite_internet_in_pilot_program
- 12 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford University Press, 2022, 97-99.
- 13 For an overview of the military techno-solutionism paradigm, see Jon R. Lindsay, “The Technology Theory of Victory,” in *Information Technology and Military Power*. Cornell University Press, 2020, 13-31.
- 14 Christopher Coker, *Future War*, 2015, Polity Press, 171-172.
- 15 See Martin C. Libicki, “Cyberwar as a Confidence Game,” *Strategic Studies Quarterly* vol. 5, no. 1, 2011, 132-147.
- 16 For an overview of the work of John Boyd, see Robert Coram, Boyd: *The Fighter Pilot Who Changed the Art of War*, Little, Brown and Company, 2002.

- 17 Although the OODA loop's origins come from air power, the concept has increasingly become important across all traditional domains of warfare. For example, see Brian R. Price, "Colonel John Boyd's Thoughts on Disruption: A Useful Effects Spiral from Uncertainty to Chaos," *Journal of Advanced Military Studies*, vol. 14, no. 1, 2023, 98-117.
- 18 Pascal Venesson, "Fighting, Fast and Slow? Speed and Western Ways of War," in Sten Rynning, Olivier Schmitt, Amelie Theussen, *War Time: Temporality and the Decline of Western Military Power*, Brookings Institution Press, 2021, 211-229.
- 19 To be sure, the OODA cycle is not only about speed. As others such as Luft and Kollars argue, it is also about tempo and timing. See Alastair Luft, "The OODA Loop and the Half-Beat," *The Strategy Bridge*, 17 March 2020 and Nina A. Kollars, "War at Information Speed: Multi-Domain Warfighting Visions," in Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 230-252. Originally found at: <https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat>
- 20 Joseph Henrotin and Stéphane Taillat, "Military Operations: What If Digital Technologies Fail on the Battlefield?," in Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 275-291.
- 21 Daniel Moore, *op. cit.*, 186-200.
- 22 Shah Zahid Khan, Mujahid Mohsin, and Waseem Iqbal, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science*, no. 7, 2021, e507.
- 23 Eduard Kovacs, "BAE Releases New Cybersecurity System for F-16 Fighter Aircraft," *Security Week*, 14 October 2022. Originally found at: <https://www.securityweek.com/bae-releases-new-cybersecurity-system-f-16-fighter-aircraft/>
- 24 Kim Hartmann and Keir Giles, "UAV Exploitation: A New Domain for Cyber Power," 8th International Conference on Cyber Conflict: Cyber Power, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 205-221.
- 25 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," *The New York Times*, 28 August 2019. Originally found at: <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>
- 26 The US National Institute of Standards and Technology (NIST)'s Cybersecurity Framework is generally used to react to cyber incidents. The NIST Cybersecurity Framework includes Identify, Protect, Detect, Respond, and Recover, and the linkages between the framework and human-centric cybersecurity and organizational culture are further explored in forthcoming work by Csenkey and Furlong.
- 27 Jon R. Lindsay, *op. cit.*, 32-70.
- 28 Jon Lindsay, *op. cit.*
- 29 Fred Kaplan, *Dark territory: The secret history of cyber war*, New York, Simon & Schuster, 2016, 68-71.
- 30 For a more in-depth history of early cyber conflict, including and beyond ELIGIBLE RECIEVER, see Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.
- 31 Comité d'éthique de la défense, *Avis sur l'environnement numérique des combattants*, ministère des armées, 13 April 2022. Originally found at: https://www.defense.gouv.fr/sites/default/files/tronc_commun/20220413_Comit%C3%A9_d%C3%A9thique_de_la_d%C3%A9fense_-_Avis_sur_l%27environnement_num%C3%A9rique_des_combattants.pdf
- 32 Brad Bigelow, "Mission Assurance: Shifting the Focus of Cyber Defence," 2017 9th International Conference on Cyber Conflict (CyCon), NATO CCD COE, 2017, pp. 1-12, <https://doi.org/10.23919/CYCON.2017.8240327>.
- 33 Airbus Defence and Space A330-200 Phénix Multi-Role Tanker Transport.
- 34 Commandement de la Cyberdéfense, *DEFNET 2024 : une cyberattaque simulée sur le plan de vol du Phénix*, Ministère des Armées, 29 March 2024. Originally found at: <https://www.defense.gouv.fr/comcyber/actualites/defnet-2024-cyberattaque-simulee-plan-vol-du-phenix>
- 35 Daniel T. Sullivan, Edward J.M. Colbert, Blaine E. Hoffman, Alexander Kott, "Best practices for designing and conducting cyber-physical-system war games," *Journal of Information Warfare*, vol. 17, no. 3, 2018, 92-105.
- 36 David Roza, "C-17 Tests Magnetic Navigation System That Works When GPS Doesn't," *Air & Space Forces Magazine*, 7 June 2023. Originally found at: <https://www.airandspaceforces.com/air-force-magnetic-navigation-gps/>
- 37 Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, Penguin Press, 2016, 147.
- 38 Diane Henshel, M. G. Cains, Blaine Hoffman & al., "Trust as a human factor in holistic cyber security risk assessment," *Procedia Manufacturing*, vol. 3, 2015, 1117-1124.
- 39 Gordon Corera, "Ukraine war: Cyber-teams fight a high-tech war on front lines," *BBC*, 5 September 2023.
- 40 *Ibid.* Originally found at: <https://www.bbc.com/news/world-europe-66686584>
- 41 Joseph Soeters, "Organizational Cultures in the Military," *Handbook of the Sociology of the Military*, Springer, 2018, 251-272.
- 42 Rebecca Slayton, "What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967-2018," *Texas National Security Review*, vol. 4, no 1, 2021.
- 43 *Ibid.*
- 44 See Michael Wayne Hankins, *The Cult of the Lightweight Fighter: Culture and Technology in the U.S. Air Force, 1964-1991*, doctoral dissertation, Kansas State University, 2018.
- 45 For a discussion of this dynamic in the aerial domain, see Michael R. Worden, *Rise of the fighter generals: the problem of air force leadership, 1945-1982*, Air University Press, 1998.
- 46 Josh Lospinoso, "Fish Out of Water: How the Military Is an Impossible Place for Hackers, and What to Do About It," *War on the Rocks*, 12 July 2018. Originally found at: <https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/>
- 47 Lee Lunn, "Cyber Operator: Are you sure you want to do that?," *The Blue Knight Review*, 2021. Originally found at: <https://www.cmrsj-rmcscj.forces.gc.ca/cb-bk/art-art/2021/art-art-2021-7-eng.asp>
- 48 Sarah P. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, doctoral dissertation, Harvard University, Graduate School of Arts & Sciences, 2019.
- 49 S. Rebecca Zimmerman, Kimberly Jackson, Natasha Lander, Colin Roberts, Dan Madden, Rebeca Orrie, *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services*, RAND Corporation, 25 February 2019.
- 50 Nicholas Romanow, "Leadership, Culture, and the Military Cyber Workforce," *War on the Rocks*, 11 April 2024. Originally found at: <https://warontherocks.com/2024/04/leadership-culture-and-the-military-cyber-workforce/>
- 51 *Ibid.*
- 52 Air Force Recruiting Public Affairs, "Cyber Direct Commissioning Program enhancement to onboard future cyber officers," US Air Force, 19 April 2023. Originally found at: <https://www.af.mil/News/Article-Display/Article/3368057/cyber-direct-commissioning-program-enhancement-to-onboard-future-cyber-officers/>
- 53 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, Oxford University Press, 2022, 75-79.
- 54 Department of National Defence, *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, 9 April 2024. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html>
- 55 Maxime Cliché, *Canadian Air Defence Sector introduces new cloud-based command-and-control system*, North American Aerospace Defense Command, 26 January 2024. Originally found at: <https://www.norad.mil/Newsroom/Article/3657967/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-syst/>
- 56 Aaron D'Andrea, "Canada's military facing 'death spiral' on recruitment, minister says," *Global News*, March 7, 2024. Originally found at: <https://globalnews.ca/news/10341588/canadian-forces-recruitment-death-spiral/>
- 57 Kristen Csenkey and Nina Bindel, "Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat," *Journal of Cybersecurity* vol. 9, no. 1, 2023, 1-14, <https://doi.org/10.1093/cybsec/tyad001>.