**CyCon 2024: Over the Horizon**
**16th International Conference on Cyber Conflict**
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

# Unity or Coherence: Shaping Future Civil-Military Intelligence Collaboration in the Cyber Domain

**Neil Ashdown**
Centre for Doctoral Training in Cyber Security
Royal Holloway, University of London
London, United Kingdom
neil.ashdown.2019@live.rhul.ac.uk

**Abstract:** Western militaries and governments are coming to recognize that they can only address the challenges of cyber defence by working with private sector cyber intelligence actors. It is almost certain that the involvement of the private sector in cyber defence will continue to expand in Western societies. Governments and militaries will therefore face the challenge of adapting to a world where – in the cyber domain – the state is not the sole provider of intelligence or security. Looking over the horizon, the paper considers two scenarios for the future of intelligence collaboration in the cyber domain within Western societies. In both scenarios, states aim to promote collaboration between industry, government, and the military, but the methods used differ. In the first scenario, Western states impose a unified structure for collaboration. In the second scenario, states aim for coherence, with governments seeking not to impose unity but to manage difference. The paper argues that the second approach is likely to be more successful but that it will require both a willingness to accept change and people able to act as translators between different organizations.

**Keywords:** *intelligence, civil, military, unity, coherence, collaboration*

# 1. INTRODUCTION

Western militaries and governments are coming to recognize that they can only address the challenges of cyber defence by working with private sector cyber intelligence actors. Deputy Commander UK Strategic Command Lt. Gen. Tom Copinger-Symes said in a September 2023 interview that in the cyber domain the UK military works with industry 'literally the whole time'. Lt. Gen. Copinger-Symes also emphasized the value of private-sector cyber intelligence for the military:

> We're very proud of how much cyberthreat data we gather as Defence, but that's tiny compared with what Microsoft gathers every day of the week … I mean, it's awesome, the scale they work at. (Martin 2023)

His comments underline two interconnected dynamics: the emergence of parts of the private sector as cyber intelligence actors and the importance of private sector cyber intelligence for modern militaries. Together, these dynamics raise the increasingly urgent question of how militaries can most effectively collaborate with industry.

The focus of this account is on the UK and the US, but a key argument of this paper is that cyber intelligence is a highly transnational practice, with the salient lines of division existing not at the country level but between groups of countries that share core values. This position has been made explicit by technology companies with advanced cyber intelligence capabilities responding to the Russia–Ukraine war (Smith 2022; Landau 2022). This account is therefore offered as a high-level description of the functioning of commercial cyber intelligence as it will be encountered by NATO militaries.

In the twenty-first century, parts of the private sector, through their access to data and their technical capabilities, have become important intelligence actors in the cyber domain (Work 2020; 2023; Zegart 2020; Healey and Korn 2019; Warner 2014). It is beyond the scope of this paper to debate whether this marks an unprecedented shift – in which, as Matthew Hurley argues, private companies can now 'conduct activities formerly the exclusive province of a state's security apparatus' – or, instead, the continuation of a long tradition of intelligence activity beyond the state (Hurley 2012, 18–19; Andrew 2018). What is key for this paper is that some of the activities that private sector organizations describe as 'cyber intelligence' are genuine intelligence activities rather than activities that approximate intelligence activity understood to be the preserve of state actors (Lindsay 2020; Stout and Warner 2018). The significance of this development remains underappreciated in discussions of cyber policy and strategy (Work 2023). It has also provoked important conceptual questions for practitioners in the private sector (Guerrero-Saade 2015).

This paper first describes private sector cyber intelligence and the networks of public and private actors that produce, exchange, and consume cyber intelligence. It then looks over the horizon, setting out two scenarios for the future organization of cyber intelligence collaboration between militaries and the private sector. The key difference will be between approaches that emphasize unity and those that emphasize coherence. These scenarios are followed by a discussion and a conclusion.

## 2. COMMERCIAL CYBER INTELLIGENCE

Organizational definitions of 'cyber intelligence' vary widely across the public and private sector (Work 2020; Bonfanti 2018; Bellaby 2016). These differences are a predictable consequence of organizations seeking to adopt definitions that align with their own histories, working practices, and ambitions (Slayton 2021; Lindsay 2020; Wiener 2016). These tendencies can be seen in various NATO member militaries' past attempts to integrate 'cyber intelligence' as a term into the established terminology of the intelligence collection disciplines, analytic practices, and military functions (Wiener 2016; Mattern et al. 2014; Hurley 2012; Neal-Hopes 2011). These challenges are not unique to the public sector; private sector organizations face similar challenges in defining cyber intelligence, while commercial pressures and marketing requirements shape how the term is applied (Work 2020; Bonfanti 2018).

Bonfanti offers a deliberately broad definition of cyber intelligence that is organizationally agnostic:

> [The term] cyber intelligence is used to convey the idea of widely scoped and better qualified knowledge of actual or potential events regarding cyberspace that may endanger an organization. (Bonfanti 2018, 107)

A broad definition can encompass the heterogeneity of cyber intelligence as a phenomenon (Work 2023; 2020; Kalkman and Wieskamp 2019). This heterogeneity is unsurprising given that, as JD Work argues, commercial cyber intelligence emerged in a 'complex and varied environment' (Work 2020, 279). It can be observed at the level of the people who work in private sector cyber intelligence, the range of cyber intelligence companies and functions, and the sharing networks that those people and organizations form, as well as in the role of cyber intelligence within the wider cyber ecosystem. This heterogeneity is important – it is a feature of commercial cyber intelligence rather than a bug.

Heterogeneity can be seen in the range of backgrounds and educations of people who work in commercial cyber intelligence. Former government and military personnel are a crucial recruiting pool for commercial cyber intelligence (Healey and Korn 2019; Petersen and Tjalve 2018). However, these former public servants work alongside people who have experience in different parts of the private sector or who are entering the workplace for the first time. These teams bring together a diverse range of skills, ranging from in-depth technical expertise to foreign languages and cultural expertise.

Cyber intelligence teams tend to be divided between technical and strategic functions (Chismon and Ruks 2015). This is by necessity, as it is rare for a single person to have the education and experience to be both a malware reverse engineer and an expert on geopolitics. This division of expertise can also be seen in CyCon's separation of technical and policy tracks. As with CyCon's focus on collaboration, effective cyber intelligence functions are those that can sustain collaboration between people with different forms of expertise.

Commercial cyber intelligence exists in a range of forms. These include organic intelligence functions within companies; vendors that provide cyber intelligence products and services; and intelligence service functions within cloud service providers (Work 2023). These companies and other cyber intelligence actors, in turn, form heterogeneous intelligence networks, sharing intelligence and collaborating in a range of public and non-public forums, as part of a community that '[spans] public and private domains' (Work 2020, 279). Highlighting the heterogeneity of these arrangements, Kalkman and Wieskamp identify four types of cyber intelligence networks: centralized networks, business networks, operational networks, and local networks (Kalkman and Wieskamp 2019, 4). The role of large transnational technology companies in the sector means that these networks also transcend state boundaries.

Cyber intelligence networks are, in turn, part of the broader 'cyber ecosystem' (Ensor 2022). Bonfanti describes this ecosystem as the '(not-formalized) international cybersecurity community that consists of representatives from supranational institutions and agencies, domestic public bodies, private organizations, and academia' (Bonfanti 2018, 105). Cyber intelligence networks therefore bring together actors that 'differ in terms of their history, activities, governance structure, communication frequency, goal consensus, member commitment, and perceived results' (Kalkman and Wieskamp 2019, 4). This heterogeneity creates multiple challenges, including differences in interests; in attitudes towards classification, ethics, and legal responsibility; in working practices; and in the use of language (Kalkman and Wieskamp 2019; Miller 2010). From the level of the individual up to the ecosystem, cyber intelligence is defined by two characteristics – heterogeneity and the importance of collaboration between different actors.

# 3. TWO SCENARIOS FOR FUTURE COLLABORATION

As indicated in the quotation from Lt. Gen. Copinger-Symes at the beginning of this paper, militaries are recognizing that the private sector has important cyber intelligence capabilities and that making the best use of these capabilities requires a close working relationship. This section outlines two scenarios for the future of this civil-military cyber intelligence collaboration. Greater collaboration between militaries and the private sector is the goal in both scenarios. Where the two scenarios differ is in the approach taken to achieving this collaboration. This paper proposes a distinction between approaches that emphasize unity and those that emphasize coherence. In the former, collaboration is advanced by one actor that imposes forms of organization, concepts, and language on other actors in this space. In the latter, actors seek instead to manage differences between themselves in a process that relies on people (here termed 'translators') who can work across different organizations and enable such interaction.

## *A. The Difference Between Unity and Coherence*

The difference between unity and coherence can be seen in NATO standardization processes. The goal of these processes is not to eliminate differences in the equipment and procedures of NATO militaries but to manage these differences to enable effective collaboration:

> Interoperability is not centrally about the elimination of difference among national militaries and the production of a monolithic transnational NATO military. Rather, it is about coordinating difference and making it manageable, organizing bodies and materials in ways that produce new capacities. (Dittmer 2017, 81)

Pursuing coherence rather than unity requires a degree of comfort with ambiguity and a recognition that it is possible to collaborate with actors whose interests intersect – but do not fully align – with our own. This comfort with ambiguity and emphasis on working with and through partners resembles, to some extent, the mindset of counterinsurgency or intelligence (Healey 2020). By contrast, an approach aimed at unity seeks to impose order and 'eliminate ambiguity' (Kramer, Butler, and Lotrionte 2017, 14).

The UK's Industry 100 (i100) scheme is an example of collaboration through 'coherence'. Under the i100 scheme, individuals from industry and academia can work with the National Cyber Security Centre (NCSC) on secondment. The NCSC is a 'unique construct' that has been described as the 'Switzerland of Cyber' – a place 'where competitors from the private sector come together with government staff, on neutral territory' (W 2022). The impetus for the creation of i100 came not from the NCSC but from a senior business leader in the private sector who presented the proposal to the NCSC and offered to provide funding (Ashdown 2024, forthcoming). In a similar vein, the NCSC operates a workspace on the popular collaboration platform Slack for UK cyber defenders. That workspace was originally created as a grassroots platform for discussion by a business leader in the private sector before it was handed over to the NCSC to operate (Ashdown 2024). The organic development and transformation of these initiatives, as opposed to their creation and enforcement by the state, evinces an approach that aims at coherence rather than unity.

### *B. Scenario 1: Unity*

In this scenario, over the next decade, Western governments will impose forms of organization on the private sector in a primarily top-down approach. The state adopts a coordinating role, creating the structures through which collaboration is permitted and required to take place. The emphasis is on the private sector coming to the public sector rather than vice versa. In this scenario:

- Collaboration between militaries and cyber intelligence providers is presented as overriding those companies' own interests. This approach is presented publicly as necessary to enable effective action on a matter of national security and defence.
- This coordinating role places greater emphasis on the state to be able to identify relevant actors, coordinate their activity in real time, and adapt to rapidly changing circumstances. The organized actors may also at times resist or struggle to fulfil their designated roles.
- As the coordinating actor, the state imposes conceptual frameworks and terminology on the private sector. Given the familiarity of militaries with establishing doctrine and training people at scale, these frameworks are likely to be primarily military in origin.
- The government and the military prioritize the development of in-house capability through strategies aimed at recruiting and retaining talent out of universities or from industry.
- Institutional arrangements are created that enable military personnel to dictate action to the private sector in times of war or crisis. More broadly, a top-down, unified approach establishes clear lines of responsibility between civil and military actors.

### *C. Scenario 2: Coherence*

In this scenario, Western governments do not dictate the form of civil-military cyber collaboration but instead encourage the development of a heterogeneous ecosystem. Rather than central coordination, this approach emphasizes decentralized social networks and emergent forms of organization. Government and military actors still operate top-down hierarchical structures for civil-military collaboration, but they coexist with alternative forms of organization. In this scenario:

- Collaboration takes place through the interlacing of multiple motives, including not only a desire to act in the interest of national security but also financial, reputational, and academic motives, among others.
- Personal relationships and trust are key to the working of this ecosystem. Much of the work falls on people who can act as 'translators' between different groups (see below).
- Without a single central authority dictating practices, frameworks, and terminology, a more complicated situation arises, with different groups adopting different approaches and language to tackle similar issues. Enabling cooperation between these groups is a key role of the translators described above.
- In this scenario, the movement of people from the public to the private sector is seen less as a retention challenge and more as an opportunity to seed the ecosystem with talent and to build personal connections into industry.
- The heterogeneity of commercial cyber intelligence is maintained in this scenario, in which collaboration takes place through surprising and novel organizational constructs and forums, often driven by industry participants rather than by the government or the military. However, this heterogeneity complicates efforts to clearly delineate roles and responsibilities between the state and private actors. Attempts to impose central coordination in times of crisis or conflict will partly rely on ad hoc cooperation rather than the activation of pre-existing lines of command.

The key differences between these two scenarios are set out in Table I below.

**TABLE I:** COMPARING SCENARIOS – UNITY AND COHERENCE

| Unity | Coherence |
|---|---|
| National security drives collaboration | Multiple motives for collaboration |
| State plays key coordinating role | Social networks play key coordinating role |
| Adoption of standard frameworks | Translation between frameworks |
| Retention of trained personnel | Movement encouraged to develop ecosystem |
| Clarity over roles and responsibilities | Reliance on ad hoc cooperation |

## 4. DISCUSSION

There are advantages and disadvantages to each aspect of the two scenarios set out above. The following discussion section will weigh some of these competing points, to underline why a coherence-focused approach is ultimately preferable for civil-military collaboration in cyber intelligence. Finally, it will highlight the tendency for advocates of the unity approach to adopt the language of coherence.

### *A. Cognitive Dispersion versus Productive Ambiguity*

A key advantage of the unity approach is that by imposing one set of conceptual frameworks, it overcomes the challenges of collaboration between people with 'very different mental models, jargon, and methodological approaches' (Vogel et al. 2017, 173). The claim that unity in terminology is necessary for effective collaboration in the cyber domain has been advanced by senior academics and practitioners (Neal-Hopes 2011; Lin 2020). Neal-Hopes uses the biblical story of Babel – a city whose people were condemned to speak different languages – as an analogy to argue for the unification of terminology:

> Unfortunately, the language of cyber space is a contemporary city of Babel…. The lack of a common lexicon detailing cyber's roles is producing cognitive dispersion at a time when the efficient expansion and aggregation of cyber forces demands cohesion. (Neal-Hopes 2011, 39)

An advocate of the coherence approach would argue that there is an important difference between shared understanding and imposing a single organization's terminology. The former is necessary for effective collaboration; the latter is likely to be counterproductive. As an example of this dynamic, the term 'open source' can refer to unclassified information or to software with public source code. This is exactly the kind of term that produces misunderstandings in collaborations between intelligence practitioners and technical experts (Vogel et al. 2017). However, attempting to enforce unity in the use of the term would be unhelpful. What matters is that people understand what their collaborators mean when they use the term.

It is entirely possible for a military cyber defence unit to work with a civilian contractor without both having to adopt explicitly military terminology, such as 'kill chain' (Hutchins, Cloppert, and Amin 2011). This may even bring benefits. As Miller observes, 'The military and intelligence establishments use words and concepts that … often tend to be misconstrued or misinterpreted by those outside their circle' (Miller 2010, 696). Moreover, all use of language encodes implicit ideas that may prematurely circumscribe the possibilities of collaboration between actors (Slayton 2021; Branch 2020). Insisting that all activity in cyberspace can only be accurately described through the language of warfare is likely to prove counterproductive if the goal is to encourage effective collaboration with the private sector (Slayton 2021; Gravell 1998). However, it also precludes the possibility of drawing on frameworks and terminology from a range of different areas, from both government and the private sector. Organizations capable of tolerating such ambiguity find themselves not with cognitive dispersion but rather with a broader range of conceptual tools with which to approach complex and unfamiliar problems.

### *B. The Need for Translators versus the Benefits of Centralization*

Adopting a coherence approach therefore puts a premium on the work of people who can act as mediators – or 'translators' – between different organizations and cultures, helping those groups to engage productively with each other. Explaining differences between professional lexicons is one part of this role, but it also involves negotiating issues of difference and identity within organizations more broadly. Effective collaboration entails changes in ways of thinking and acting among all the parties involved. Translators are individuals who, through their interactions and movements across organizational boundaries, facilitate these productive transformations (Ashdown 2024).

The importance of translators is well understood, and they appear in a variety of guises across the literature. Harknett and Stever note approvingly that 'dual-hatted' officials who sit in different institutional contexts can provide 'greater synergy of perspective' (Harknett and Stever 2009, 7). Vogel et al. describe the importance within cross-organizational teams of 'human enablers' 'who can advise on how to work best collaboratively' (Vogel et al. 2017, 178). Trent emphasizes the importance of 'spanners and brokers' who can work across organizations, 'moving ideas and building new communities'; he emphasizes that spanners are 'people with (or willing to develop) first-hand experience in multiple domains' (Trent 2018, 120).

However, this is not an easy role to play, and a coherence approach places a substantial burden on these translators (Ashdown 2024). It is for this reason that the unity approach reflects a preference for collaboration to be centralized and managed at a higher level rather than depending on social networks and professional relationships. The goal is 'to transcend the dependence on individual personal/professional relationships which are, to an extent, transient' (Piazza, Vasudevan, and Carr 2023, 11). A centralized approach has the advantage of reducing the burden on the people whose personal relationships currently maintain networks of collaboration in public and private cyber intelligence. However, as will be argued below, the risk is that in centralizing control, much of the benefit of those informal, haphazard, but productive connections will be lost.

### *C. Tensions Between Motives for Collaboration*

Collaboration on cyber intelligence makes the private sector an active participant in the cyber defence of military networks, in a way that Lt. Gen. Copinger-Symes argues differs from the traditional defence procurement relationship, 'where ultimately industry partners hand over a tank and then we operate the tank' (Martin 2023). Such relationships are an example of the kind of 'operational intimacy' between public and private actors that, it is argued, will be required to strengthen cyber security (Inglis and Krejsa 2022; Pell 2022; Landau 2022). However, such active engagement and proximity to operational military activity by private sector actors raises policy, legal, and ethical questions and challenges core ideas about the primacy of the state in matters of defence (Carr 2016; Miller 2010; Abrahamsen and Williams 2010).

The unity approach simplifies some of these questions – although it does not resolve them – by creating clear lines of control and responsibility for private actors. In this scenario, the reason private actors collaborate with the state on cyber defence is that they are mandated to do so in the national interest (Harknett and Stever 2009; Kramer, Butler, and Lotrionte 2017; Carr 2016). Some advocates of this approach have proposed creating nascent command structures for the private sector that can be activated in times of crisis or conflict (Kramer, Butler, and Lotrionte 2017). By contrast, in the coherence scenario it is much more challenging to see how different actors' interests are aligned and where they differ, and where the divisions between roles and responsibilities lie.

The challenge with the unity approach is that it risks casting the private sector as a passive intermediary rather than as a diverse set of actors with their own interests and motives. For example, Harknett and Stever's discussion of the benefits of greater public–private collaboration portrays non-state actors as impersonal bodies that are 'to be mobilized' and that must 'submit and participate' in the federal government's initiatives (Harknett and Stever 2009, 2, 10). They argue that public concern over privacy should be downplayed in favour of 'the more important issue of the general population's responsibility to government' (Harknett and Stever 2009, 2). Similar perspectives are visible in the claim that an effective 'whole of society' approach requires the private sector to 'adjust to a paradigm shift … where national security concerns must be elevated above corporate interests' (Williams 2023, 3). Such terminology treats other actors in the network as intermediaries that must be aligned with the state's interests. The goal is 'more subordination than alliance' (Healey 2020, 93). As noted above, these arguments address pressing questions about the organization of civil-military cooperation in the cyber domain. Yet the way they are articulated precludes further discussion. Rather than encouraging debate, they announce a conclusion that another actor has failed properly to internalize.

### *D. The Risk of Pursuing Unity in a Heterogenous, Collaborative Ecosystem*

Crucially, even if we accept these arguments about national security, blunt statements of necessity may not be the best way to promote willing collaboration. Research suggests that cyber intelligence networks that emerged in a 'bottom-up' fashion are perceived by their members as producing better results (Kalkman and Wieskamp 2019, 11, 19–20). Similarly, an analysis of cyber intelligence and security collaboration in the US notes:

> The sharing of threat intelligence information based on current threat activity is … embraced in the private sector. This sharing is not bound by a common framework or lexicon and is driven by private cybersecurity companies. (Bronk and Conklin 2022, 161)

This is the fundamental point about cyber intelligence that argues for an approach aimed at coherence. Analysis of innovative technological ecosystems suggests that they develop through risk-taking, cooperation, and social networks rather than through 'hierarchical organizations, vertical information flow, and centralized decision-making' (Trent 2018, 117–18). With a capability as specialized, transnational, and fundamentally collaborative as cyber intelligence, any attempt to impose unity risks undermining the very capability it seeks to mobilize. In this vein, Healey and Korn argue that calls for the private sector to work under US government control 'may be counterproductive':

> The main goal of the coordination of all of these defensive efforts … is not unity of command centered on [the US Department of Defense], but unity of effort, unity of action, and loose coordination to keep independent groups working toward the same goal. (Healey and Korn 2019, 235)

Such an approach would mean that the Department of Defense would exercise less control and that defence would be less well coordinated – 'but this is a small loss to achieve better synchronization across all defense, in both the public and private sectors' (Healey and Korn 2019, 235). Preserving what makes cyber intelligence valuable requires an approach that can accept variation and ambiguity, one that seeks coherence rather than unity. Adopting such an approach will be challenging. It will require organizations to embrace productive ambiguity rather than fearing cognitive dispersion; to trust in individual social networks and translators as well as hierarchical structures; and to respect the diverse set of motives that might lead people and organizations to collaborate. However, the advantages of this approach outweigh these challenges.

# 5. CONCLUSION

The production and use of cyber intelligence, and the practice of cyber security more broadly, involves bringing together complex networks of people, processes, and technologies in a way that is fundamentally innovative and collaborative (Kalkman and Wieskamp 2019). This presents a challenge for NATO militaries, as they increasingly collaborate with the private sector in this area. Civil-military collaboration on cyber intelligence will play out in multiple ways simultaneously, through contractual arrangements, intelligence sharing platforms and forums, the movement of individuals between careers, and informal personal connections between individuals. NATO militaries will need to adapt to working in unfamiliar ways with an important new set of partners. In this regard, Healey and Korn call into question 'the default assumption of military cyber defenders that, to defend the Nation, they must take control of the assets themselves' (Healey and Korn 2019, 231). Overcoming that 'default assumption' – the desire to impose unity rather than live with ambiguity and difference – will be crucial for effective military collaboration with the private sector.

Highlighting the need for change, Chris Inglis and Harry Krejsa call for 'a new social contract for the digital age – one that meaningfully alters the relationship between public *and private sectors and proposes a new set of obligations for each'* (Inglis and Krejsa 2022, emphasis added). Such calls should always be viewed with some caution. The goal of coherence is a naturally appealing one, particularly in cyber security. The idea that digital technologies necessitate novel approaches, particularly ones that are perceived as more agile and decentralized, has been formative in understandings of the cyber domain (Arquilla and Ronfeldt 1993). The attractiveness of this idea means there is a risk that people will use the language of 'coherence' to describe approaches to managing civil-military collaboration that fall back on 'unifying' practices of centralization and control.

A foreseeable consequence of genuine collaboration will be a transformation of *all* the organizations involved, public and private. Vogel et al. argue that the key to effective collaboration between academia, industry, and the intelligence community is 'organizational innovation and adaption' (Vogel et al. 2017, 174). This process of transformation is something that militaries have at times opposed, as seen, for example, in resistance to lowering physical fitness requirements for personnel working in cyber roles (Lin 2020, 97). In his September 2023 interview, Lt. Gen. Copinger-Symes described the creation of the UK National Cyber Force – a novel organization bringing together Defence and the intelligence agencies in a way that has required changes for all participants. Lt. Gen. Copinger-Symes described this as a process of 'bending ourselves out of shape together' (Martin 2023). This image captures the essence of the transformative nature of collaboration – different entities coming together, with a willingness to productively manage difference and, in doing so, to develop new capacities (Dittmer 2017).

Theorists of cyber conflict suggest we can learn from studying the development of concepts and operational art around earlier novel domains such as the air and the sub-surface (Neal-Hopes 2011; Hurley 2012; Perkovich and Levite 2017). However, the value of historical study may be as much in examining the process by which multiple actors collectively (but not always cooperatively) defined those new domains and their roles within them. In doing so, those actors redefined themselves – they 'bent themselves out of shape together'. It is precisely such a process of redefinition that will play out as militaries and private sector actors learn how to collaborate in the production, sharing, and use of cyber intelligence. The choice facing these organizations is whether to pursue coherence and bend, or cling to unity and break.

## REFERENCES

Abrahamsen, Rita, and Michael C. Williams. 2010. *Security beyond the State: Private Security in International Politics*. Cambridge University Press.

Andrew, Christopher. 2018. *The Secret World: A History of Intelligence*. Penguin UK.

Arquilla, John, and David Ronfeldt. 1993. 'Cyberwar Is Coming!' *Comparative Strategy* 12 (2): 141–65.

Ashdown, Neil. 2024. 'Advocates of Collaboration: Assembling Cyber Intelligence in the UK'. PhD Thesis, Royal Holloway University of London.

Bellaby, Ross W. 2016. 'Justifying Cyber-Intelligence?' *Journal of Military Ethics* 15 (4): 299–319. https://doi.org/10.1080/15027570.2017.1284463.

Bonfanti, Matteo E. 2018. 'Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice'. *Cyber, Intelligence, and Security* 2 (1): 105–21.

Branch, Jordan. 2020. 'What's in a Name? Metaphors and Cybersecurity'. *International Organization*, September, 1–32. https://doi.org/10.1017/S002081832000051X.

Bronk, Chris, and Wm Arthur Conklin. 2022. 'Who's in Charge and How Does It Work? US Cybersecurity of Critical Infrastructure'. *Journal of Cyber Policy* 7 (2): 155–74. https://doi.org/10.1080/23738871.2022.2116346.

Carr, Madeline. 2016. 'Public–Private Partnerships in National Cyber-Security Strategies'. *International Affairs* 92 (1): 43–62. https://doi.org/10.1111/1468-2346.12504.

Chismon, David, and Martyn Ruks. 2015. *Threat Intelligence: Collecting, Analysing, Evaluating*. MWR InfoSecurity.

Dittmer, Jason. 2017. *Diplomatic Material: Affect, Assemblage, and Foreign Policy*. Duke University Press.

Ensor, Chris. 2022. 'NCSC View: Future Ecosystem Challenges'. NCSC. 1 November 2022. https://www.ncsc.gov.uk/search.

Gravell, William. 1998. ‘Some Observations Along the Road to National Information Power Symposium: International Information Infrastructure Protection and National Security’. *Duke Journal of Comparative & International Law* 9 (2): 401–26.

Guerrero-Saade, Juan Andrés. 2015. ‘The Ethics and Perils of APT Research: An Unexpected Transition into Intelligence Brokerage’. In *Proceedings of the 25th Virus Bulletin International Conference*. http://media.kaspersky.com/pdf/Guerrero-Saade-VB2015.pdf.

Harknett, Richard J., and James A. Stever. 2009. ‘The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen’. *Journal of Homeland Security and Emergency Management* 6 (1). https://doi.org/10.2202/1547-7355.1649.

Healey, Jason, and Erik B. Korn. 2019. ‘Defense Support to the Private Sector: New Concepts for the DoD’s National Cyber Defense Mission’. *The Cyber Defense Review*, 227–44.

Healey, Jason. 2020. ‘A Bizarre Pair: Counterinsurgency Lessons for Cyber Conflict’. *Parameters* 50 (3): 85–94.

Hurley, Matthew M. 2012. ‘For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance’. *Air & Space Power Journal* 26 (6): 12–33.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. 2011. ‘Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains’. *Leading Issues in Information Warfare & Security Research* 1 (1): 80.

Inglis, Chris, and Harry Krejsa. 2022. ‘The Cyber Social Contract’. *Foreign Affairs*, 21 February 2022. https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract.

Kalkman, Jori Pascal, and Lotte Wieskamp. 2019. ‘Cyber Intelligence Networks: A Typology’. *The International Journal of Intelligence, Security, and Public Affairs* 21 (1): 4–24. https://doi.org/10.1080/23800992.2019.1598092.

Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. 2017. ‘Cyber and Deterrence’. Atlantic Council. 3 January 2017. https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-and-deterrence/.

Landau, Susan. 2022. ‘Cyberwar in Ukraine: What You See Is Not What’s Really There’. Default. 30 September 2022. https://www.lawfaremedia.org/article/cyberwar-ukraine-what-you-see-not-whats-really-there.

Lin, Herbert. 2020. ‘Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts’. *The Cyber Defense Review* 5 (2): 89–108.

Lindsay, Jon R. 2020. ‘Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem’. *Intelligence and National Security*, October 2020. http://www.tandfonline.com/doi/abs/10.1080/02684527.2020.1840746.

Martin, Alexander. 2023. ‘British Army General Says UK Now Conducting “Hunt Forward” Operations’. 25 September 2023. https://therecord.media/uk-hunt-forward-operations-lt-gen-tom-copinger-symes.

Mattern, Troy, John Felker, Randy Borum, and George Bamford. 2014. ‘Operational Levels of Cyber Intelligence’. *International Journal of Intelligence and CounterIntelligence* 27 (4): 702–19. https://doi.org/10.1080/08850607.2014.924811.

Miller, Bowman H. 2010. ‘Soldiers, Scholars, and Spies: Combining Smarts and Secrets’. *Armed Forces & Society* 36 (4): 695–715. https://doi.org/10.1177/0095327X10361667.

Neal-Hopes, Timothy. 2011. ‘“Preventing a Cyber Dresden”: How the Evolution of Air Power Can Guide the Evolution of Cyber Power’. Master’s thesis, School of Advanced Air and Space Studies. https://apps.dtic.mil/sti/pdfs/AD1019450.pdf.

Pell, Stephanie. 2022. 'Private-Sector Cyber Defense in Armed Conflict'. *Lawfare*, 1 December 2022. https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict.

Perkovich, George, and Ariel Levite, eds. 2017. *Understanding Cyber Conflict: 14 Analogies*. Washington, DC: Georgetown University Press.

Petersen, Karen Lund, and Vibeke Schou Tjalve. 2018. 'Intelligence Expertise in the Age of Information Sharing: Public–Private "Collection" and Its Challenges to Democratic Control and Accountability'. *Intelligence and National Security* 33 (1): 21–35. https://doi.org/10.1080/02684527.2017.1316956.

Piazza, Anna, Srinidhi Vasudevan, and Madeline Carr. 2023. 'Cybersecurity in UK Universities: Mapping (or Managing) Threat Intelligence Sharing within the Higher Education Sector'. *Journal of Cybersecurity* 9 (1): tyad019. https://doi.org/10.1093/cybsec/tyad019.

Slayton, Rebecca. 2021. 'What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018'. *Texas National Security Review*, 11 January 2021. http://tnsr.org/2021/01/what-is-a-cyber-warrior-the-emergence-of-u-s-military-cyber-expertise-1967-2018/.

Smith, Brad. 2022. 'Defending Ukraine: Early Lessons from the Cyber War'. Microsoft On the Issues. 22 June 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Stout, Mark, and Michael Warner. 2018. 'Intelligence Is as Intelligence Does'. *Intelligence and National Security* 33 (4): 517–26. https://doi.org/10.1080/02684527.2018.1452593.

Trent, Stoney. 2018. 'Cultivating Technology Innovation for Cyberspace Operations'. *The Cyber Defense Review* 3 (3): 115–34.

Vogel, Kathleen M., Jessica Katz Jameson, Beverly B. Tyler, Sharon Joines, Brian M. Evans, and Hector Rendon. 2017. 'The Importance of Organizational Innovation and Adaptation in Building Academic–Industry–Intelligence Collaboration: Observations from the Laboratory for Analytic Sciences'. *The International Journal of Intelligence, Security, and Public Affairs* 19 (3): 171–96. https://doi.org/10.1080/23800992.2017.1384676.

W, Ollie. 2022. 'Inside Industry 100 - the on-Loan CTO'. NCSC.GOV.UK. 22 April 2022. https://www.ncsc.gov.uk/blog-post/inside-industry-100-the-on-loan-cto.

Warner, Michael. 2014. *The Rise and Fall of Intelligence: An International Security History*. Georgetown University Press. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=766382&site=ehost-live.

Wiener, Craig. 2016. 'Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation'. PhD thesis, George Mason University.

Williams, B. K. 2023. *Public-Private Bonhomie May Not Last Amid Strategic Competition*. Livermore, CA: Lawrence Livermore National Laboratory (LLNL).

Work, J. D. 2020. 'Evaluating Commercial Cyber Intelligence Activity'. *International Journal of Intelligence and CounterIntelligence* 33 (2): 278–308. https://doi.org/10.1080/08850607.2019.1690877.

———. 2023. 'Private Actors and the Intelligence Contest in Cyber Conflict'. In *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, edited by Robert Chesney and Max Smeets, 225–60. Georgetown University Press. https://books.google.co.uk/books?id=ZHmbEAAAQBAJ.

Zegart, Amy. 2020. 'Intelligence Isn't Just for Government Anymore'. *Foreign Affairs*, 5 November 2020. https://www.foreignaffairs.com/articles/united-states/2020-11-02/intelligence-isnt-just-government-anymore.