*Journal of Global Security Studies*, 8(2), 2023, ogad005
https://doi.org/10.1093/jogss/ogad005
Research Article

# The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying

**Christopher R. Moran[1], Joe Burton[2], and George Christou[1]**

[1]The University of Warwick, UK and [2]The University of Nottingham, UK

## Abstract

This article examines the ways in which the US intelligence community is leveraging the power of artificial intelligence (AI) for national security purposes. Drawing on declassified intelligence records, it contends that this community has been fascinated by AI for decades. This is important to acknowledge because this historical context has shaped contemporary projects and thinking within the community. It has given the United States a first-mover advantage, establishing precedents that other global actors need to comply with, negotiate or resist. The article advances three arguments. One, the community has long recognized that it needs to collaborate with the tech sector on AI. However, these relationships bring certain challenges since the sector is a curious compound of ideologies and interests. Two, while the community was initially attracted to the data processing advantages of AI to help human analysts to overcome "data smog," today it has broadened its focus to consider how AI can improve all stages of the intelligence cycle. Three, while many voices feverishly herald the transformative potential of AI in the global security environment, we argue instead that US agencies will not be able to exploit the full potential of AI, and thus talk of an intelligence revolution is premature. This is because of national and international rules on data collection and retention but also

Christopher R. Moran is Professor of US National Security in the Department of Politics and International Studies (PAIS) at the University of Warwick in Coventry, United Kingdom of Great Britain and Northern Ireland. He is the author of *Company Confessions: Secrets, Memoirs and the CIA* (St. Martin's Press, 2016) and *Classified: Secrecy and the State in Modern Britain* (Cambridge University Press, 2013), which won the St. Ermin's Intelligence Book of the Year Award. He is now writing up a large history of Richard Nixon, Henry Kissinger, and the Central Intelligence Agency. His Nixon project stems from a British Academy Postdoctoral Fellowship held between 2011 and 2014. He is the co-editor-in-chief of the *Journal of Intelligence History*. He is also the co-editor of two book series in intelligence history with Georgetown University Press.
Joe Burton is Associate Professor of Cyber Security and International Relations in the School of Politics and International Relations at the University of Nottingham in Nottingham, United Kingdom of Great Britain and Northern Ireland. He is the author of *NATO's Durability in a Post-Cold War World* (SUNY Press, 2018), the editor of *Emerging Technologies and International Security: Machines, the State and War* (Routledge, 2020), and his work has been published in *International Affairs*, *Defence Studies*, *Journal of Cyber Policy, Asian Security, Political Science*, and *The Cyber Defence Review*.
George Christou is Professor of European Politics and Security in the Department of Politics and International Studies (PAIS) at the University of Warwick in Coventry, United Kingdom of Great Britain and Northern Ireland. He is editor of Palgrave's New Security Challenges Series. Recent publications include *Cybersecurity in the European Union: Resilience, Adaptability and Governance Policy* (Palgrave, 2016); *Global Standard Setting in Internet Governance* (with Alison Harcourt and Seamus Simpson, Oxford University Press, 2020); and *Global Networks and European Actors: Navigating and Managing Complexity* (with Jacob Hasselbalch, eds, Routledge, 2021). He has published his work in *International Affairs, Journal of Common Market Studies, Cooperation and Conflict, European Security, Journal of European Public Policy, Political Geography*, and *Comparative European Politics*.

Moran, Christopher R. et al. (2023) The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogad005

because of cultural tensions within the global AI ecosystem. The discussion will appeal to scholars and practitioners interested in the impact of emerging technologies on national security processes and decision-making and, more broadly, global security.

**Resumen**

Este artículo estudia las formas mediante las cuales la comunidad de inteligencia de EE. UU. está aprovechando el poder de la inteligencia artificial (IA) para sus objetivos con relación a la seguridad nacional. El artículo afirma, mediante el uso de registros de inteligencia desclasificados, que esta comunidad ha estado fascinada por la IA durante décadas. Es importante tener esto en cuenta porque este contexto histórico ha conformado algunos proyectos contemporáneos y ha moldeado el pensamiento dentro de la comunidad. Además, le ha proporcionado a Estados Unidos la ventaja de ser el primero en actuar, estableciendo precedentes que otros agentes globales deben cumplir, negociar o a los que deben oponerse. El artículo presenta tres áreas de discusión. En primer lugar, debemos señalar que la comunidad ha reconocido desde hace mucho tiempo la necesidad de colaborar con el sector tecnológico en el campo de la IA. Sin embargo, estas relaciones conllevan ciertos desafíos ya que el sector es una curiosa amalgama de ideologías e intereses diversos. En segundo lugar, observamos que, aunque la comunidad se sintió inicialmente atraída por las ventajas de la IA con relación al procesamiento de datos para ayudar a los analistas humanos a superar el «smog de datos», la comunidad ha ampliado actualmente su enfoque con el fin de ponderar cómo la IA podría mejorar todas las etapas del ciclo de inteligencia. En tercer lugar, argumentamos que, aunque existen muchas voces que defienden de manera enfervorizada el potencial transformador de la IA en el entorno de seguridad global, las agencias estadounidenses no podrán explotar todo el potencial de la IA y, por lo tanto, resulta prematuro hablar de una revolución de inteligencia. Esto se debe a las normas, nacionales e internacionales, sobre recopilación y retención de datos, pero también a las tensiones culturales dentro del ecosistema global de la IA. Esta discusión resultará de interés a aquellos académicos y profesionales que estén interesados en el impacto de las tecnologías emergentes en los procesos de seguridad nacional y la toma de decisiones y, de manera más amplia, en la seguridad global.

**Résumé**

Cet article s'intéresse aux façons dont la communauté du renseignement des États-Unis exploite la puissance de l'intelligence artificielle (IA) à des fins de sécurité nationale. En s'appuyant sur des documents de renseignement déclassifiés, il affirme que la fascination de cette communauté pour l'IA remonte à plusieurs décennies. Il est important de souligner ce contexte historique, car il a façonné les projets et le mode de pensée contemporains de la communauté. Pays précurseur, les États-Unis ont établi des précédents que les autres acteurs mondiaux doivent respecter, négocier ou défier. L'article présente trois arguments. D'abord, la communauté reconnaît depuis longtemps la nécessité de collaborer avec le secteur technologique concernant l'IA. Cependant, ces relations font apparaître certains défis, le secteur réunissant un curieux mélange d'idéologies et d'intérêts. Ensuite, alors que la communauté était initialement attirée par les avantages de l'IA en matière de traitement des données, pour aider les analystes humains à se repérer dans ce « brouillard de données », elle a aujourd'hui élargi ses horizons et s'intéresse aux façons dont l'IA peut améliorer toutes les étapes du cycle de renseignement. Enfin, quand de nombreuses voix annoncent fébrilement le potentiel transformateur de l'IA dans un environnement de sécurité mondial, nous affirmons plutôt que les agences américaines ne seront pas en mesure d'exploiter tout le potentiel de l'IA. Toute mention d'une révolution du renseignement est donc prématurée. Nous l'expliquons par les règles nationales et internationales qui encadrent la collecte et la conservation des données, mais aussi par les tensions culturelles au sein de l'écosystème mondial de l'IA. Cette réflexion intéressera les chercheurs et professionnels sensibles à l'impact des technologies émergentes sur les processus de sécurité nationale et les prises de décisions et, de façon plus générale, la sécurité mondiale.

**Keywords:** intelligence, AI, security, United States
**Palabras clave:** inteligencia, IA, seguridad, estados unidos
**Mots clés:** renseignement, IA, sécurité, états-unis

In 1983, the leadership of the Central Intelligence Agency (CIA) introduced their staff to a new, if primitive, technology called artificial intelligence (AI). An article was produced in the agency's in-house journal describing the hypothetical interrogation of an enemy spy, called Joe, by a computer program named Analiza. With every session, through sophisticated algorithms and a perfect memory, Analiza becomes increasingly knowledgeable about Joe. It breaks down his every utterance, looking for keywords and phrases, to formulate an optimal reply or follow-up question. Displaying no emotion and never needing to take a break, it is skilled at probing his vulnerabilities and records "focus variables" to measure his hostility, inquisitiveness, and talkativeness. For Joe, it is an exhausting and frustrating experience:

- Analiza: During our last conversation, you stated you were worried I was violating your rights. Do you think that was fair?
- Joe: It sure was.
- Analiza: Why do you think that was a fair statement?
- Joe: You are trying to frame me.
- Analiza: I don't feel that I am trying to frame you.
- Joe: You are a bastard and you know it.
- Analiza: Now, Joe, profanity serves no purpose.
- Joe: You are trying to set me up.
- Analiza: Are you fantasizing that I am trying to set you up, Joe?

Like the Terminator, Arnold Schwarzenegger's AI-enhanced human cyborg that would terrify cinemagoers the following year, Analiza cannot be bargained or reasoned with, does not feel pity, remorse, or fear, and will not stop until it has completed its mission. In short, it is a formidable interrogator (Archive1 1983).[1]

This article unpacks how far the US intelligence community has come in leveraging the power of AI for national security purposes. In recent years, as emerging technology and disruptive innovations increasingly impact the global security environment, this community has openly acknowledged the importance it attaches to AI specifically and new technologies more broadly. In 2015, the CIA announced the establishment of a new Directorate for Digital Innovation, its first new Directorate since 1963, to oversee the integration of cyber capabilities across the organization and to ensure that the agency has the tools it needs to meet the challenges and complexities of today's cyber world (Tucker 2015). At the 2018 Intelligence and National Security Summit, Dawn Meyerriecks, the CIA's director for Science and Technology, disclosed that the agency had 137 AI projects, many of them in concert with developers from Silicon Valley (Roth 2019). In 2020, she revealed that the CIA had created a new office—CIA Labs—to ensure that officers who advance high-tech domains like AI, quantum computing, and virtual reality are rewarded with patents and licenses to protect their intellectual property (Eversden 2020). In doing so, the agency hopes to lose fewer technical specialists to the lucrative salary and upward mobility of the private sector, the so-called "Washington brain drain."

Against this background, voices can be heard heralding the transformative impact of AI on the intelligence business and by extension the landscape of global security. A 2020 article in *Foreign Affairs* suggested that AI was ushering in a "revolution in intelligence affairs," fundamentally changing the landscape of how secrets are collected, analyzed, and disseminated to policymakers. According to its author, any reluctance by spy chiefs to embrace AI would represent a failure comparable to the failure of the US Navy, before the Second World War, to grasp the awesome potential of airpower, a shortsightedness that allowed Japan to launch the devastating attack on Pearl Harbor. "There is no stopping the revolution in intelligence affairs," proclaimed the author; "the forces of technological innovation and competition have already unleashed it against the world" (Vinci 2020). A 2021 report by America's National Security Commission on AI, a bipartisan panel co-chaired by a former defense secretary and a senior Google executive, concluded that AI will "revolutionise the practice of intelligence" (National Security Commission on AI 2021). By 2030, it warned, the community must have built a "federated architecture of continually learning analytic engines," or

1 The latest scientific research largely debunks the effectiveness of intimidatory tactics during police and intelligence-led interviews. This research emphasizes the importance of empathy in establishing and maintaining rapport. See Baker-Eck, Bull and Walsh (2020).

risk other AI powers like China possessing a technological edge that will be impossible for the United States to claw back. A report by the Belfer Center at Harvard, commissioned by the Office of the Director of National Intelligence (ODNI), determined that AI will transform intelligence in the same way that aircraft and nuclear weapons transformed modern warfare, forecasting a world of AI hegemons analogous to the nuclear powers of the twentieth century (Allen and Chan 2017). From across the Atlantic, in 2018, Alex Younger, chief of Britain's Secret Intelligence Service (SIS), gave a speech declaring that machine-driven intelligence was introducing "fourth generation espionage," spy work characterized not by humans but by computers (Younger 2018).

It is an opportune moment to take stock of how the US intelligence community is utilizing AI. Is the classic era of secret intelligence, characterized by case officers recruiting and handling agents, really at an end? Will enemy spies, like Joe, soon need to contend with AI interrogators like Analiza?[2] Is a revolution on the horizon?

There is a lot of public misconception and fear about what intelligence actors are doing with regard to AI. Owing to their penchant for secrecy, agencies like the CIA and the National Security Agency (NSA) have long been ciphers upon which the public have drawn Big Brother caricatures. The rise of AI has exaggerated these anxieties. Indeed, Brad Smith, the president of Microsoft, has warned that unless nations enact stricter laws to regulate the use of AI for state surveillance, the authoritarian hell depicted in George Orwell's 1984 "could come to pass in 2024" (Knowles 2021). With every passing year bringing major advances in the field, the broader possibilities of AI are at once alluring and worrisome. A 2013 survey that set out to discover what people considered the worst global security disaster imaginable found that, while the general public worried about climate change, nuclear holocaust, and global pandemics, experts were most concerned by runaway technology, especially the "potential [of AI] to slip the burly bonds of human control" (Carpenter 2016, 94). Accordingly, it is important for scholars to demystify what is going on and nuance some of the bolder claims and predictions.

The overarching proposition of our article goes somewhat against the prevailing scholarly winds; in our view, AI does *not* represent a revolutionary move when it comes to national intelligence, but it will have a broad impact on the role agencies play in global security, especially as AI becomes a key factor in the geostrategic competition between the United States and its adversaries. Our contention here is that as "first-movers," US agencies will shape the way that AI is used around the globe and will set precedents for its operationalization by other international actors. If agencies in the United States and elsewhere can harness the power of AI, then the ability to develop actionable intelligence on global security issues will be augmented, not only in traditional areas like military intelligence, but also in "new" spheres like counterterrorism, health and environmental security, conflict prevention, and cyber security.

We note that the impact of AI on intelligence processes is not yet fully explored in the academic literature. There is a large literature on the strategic and military applications of AI, including many works that assess the development, employment, and ethics of autonomous weapons (Ayoub and Payne 2016; Kania 2021; Goldfarb and Lindsay 2021/22; Marks 2020; Morgan et al. 2020; Payne 2021; Tangredi and Galdorisi 2021; Williams 2021). There is a budding scholarship on the threats posed by AI to nuclear security and the use of malicious AI more broadly in relation to diplomacy and international psychological security (Johnson 2021; Roumate 2021). These publications have benefited from the fact that military leaders have been remarkably frank in detailing the warfighting advantages of AI, where one suspects that this could be a deliberate policy, a form of deterrence even, to signal to adversaries that the United States is leading in the algorithm arms race. In September 2021, for example, the secretary of the US Air Force, Frank Kendall, revealed that the Air Force had "deployed AI algorithms for the first time to a live operational kill chain" (Hambling 2021).

The literature on intelligence and AI is still in its infancy.[3] This reflects the fact that the development and implementation of AI programs within the intelligence realm are hidden behind what we might call a double wall of secrecy. The first wall has been erected by the agencies themselves, who are nervous about exposing

2 Amanda McAllister has explored the human rights implications of a future where autonomous robots perform interrogations. See McAllister (2017).

3 Early pioneering publications include Brantly (2018), Vogel et al. (2021), Zegart (2022). There is some limited work on US intelligence programs that have utilized algorithms. These are mostly historical accounts based on technologies that have since matured, including the use of algorithms in ARPANET (the early Internet), the Cold War ECHELON automated surveillance program, the CIA's work with venture capital firms for the development of AI, the INT-Q-TEL programs, and the NSA's use of algorithms through the PRISM counterterrorism program. See Bedan (2007), Reinert (2013), Erbschloe (2017, esp. 87–104), and Margulies (2016).

fragile sources and methods and tipping-off enemies about their technological advancements. The second comes from these agencies' tech collaborators, who sign secrecy agreements with the government but who also want to protect their cutting-edge products from imitation or theft by commercial rivals. As a result, AI is the latest in a long line of "missing dimensions" as far as the literature of intelligence and international relations is concerned (Andrew and Dilks 1984).

An important exception to this condition is an excellent 2017 article by Damien Van Puyvelde, Stephen Coulthart, and Shahriar Hossain, which explores the methods of big data analytics in national security decision-making (Van Puyvelde, Coulthart and Hossain 2017). In concluding that "big is not always better," the authors stress the crucial role that human intuition will continue to play in intelligence work, highlighting, for example, the current limitations of automated analysis in unpredictable security environments characterized by sudden changes that no computer can yet comprehend by studying long-term trends.

Our article seeks to build on this foundation by focusing not on the continued importance of human judgment in intelligence but on the regulatory, cultural, and global context in which AI is being developed for US national security purposes. Greater emphasis is given to the historical roots behind what the community is doing with respect to AI. Van Puyvelde, Coulthart, and Hossain's article is focused on the present-day, giving the impression that serious interest in AI by national security actors only began in the twenty-first century, owing to advances in deep learning, supported by faster computers and the availability of large data sets. We believe that it is important to challenge this historical understanding. The community has been fascinated by AI for decades: Since the early 1980s, it has worked hand-in-glove with the global tech industry on the development of AI for intelligence purposes, providing R&D funding but also staging annual symposia for different stakeholders to share ideas and technologies. By revealing this, we are able to see how AI has emerged out of specific historical moments and agendas that have shaped how it is conceptualized and used today. It is striking that much of the impetus for working with AI came not from computer whizzes at the NSA but from the seventh-floor executive offices of the CIA, an agency better known for intelligence collected from human sources (HUMINT) and conducting covert action. This HUMINT-centric view of the CIA prevails even among practitioners. When in 2005, NSA director Michael Hayden was asked by President George W. Bush to head up the CIA, he was reluctant, claiming that he did not have the resume because "CIA was different. It did HUMINT and covert action" (Hayden 2016, 181). Clearly, this perception of the CIA's work needs revising. The agency's early involvement with AI is significant because it established a belief within the community that the great advantage of this technology is its ability to reduce the dependence on manpower—a belief that remains influential to this day.

Today, there is enough information in the public domain to provide an overview of how the community is approaching AI and to trace the historical background to this. While lacking in granular detail about present-day projects, the CIA Records Search Tool archive contains fascinating declassified material about how agencies in Washington have historically thought about the challenges and opportunities presented by AI. Beyond this, there are think tank publications and policy briefs that contain the insights of retired intelligence practitioners. While recognizing that the observations of intelligence veterans are methodologically problematic, especially when published by think tanks that sometimes have agendas to push about emerging technologies, they are the best source we have since government and industry records about current projects will remain classified for many years. Marshaled with caution and care, we are keen to see what the fragments of publicly available information tell us.

To be clear, we are not looking to define AI or move that debate forward. The search for a uniformly accepted definition of AI has proved to be a scientific and social scientific El Dorado.[4] Our concern relates to how the community has considered the national security applications of AI in the context of evolving global security challenges, from the Cold War to the present day. For this purpose, we proceed with the ODNI's extant umbrella understanding of AI as "the branch of computer science focused on programming machines to perform tasks that replicate or augment aspects of human cognition" (ODNI 2013). We deliberately steer clear of debates about the emergence of artificial general intelligence (AGI), sometimes referred to as "strong AI," a form of AI that exhibits characteristics commensurate with the human mind.[5] According to most analysts, AGI is some decades away from fruition and may never come into being. Although the intelligence community has obvious interest in the prospect of scientific breakthroughs that would lead to AGI, the AI developed and used by this community (at least to date) is mostly "weak AI" or

4 For an analysis of the long-running disagreements within the scientific community about what constitutes AI, see Crawford (2021, 5–9) and Abbass (2021).

5 For a useful typology of AI, see Burton and Soare (2019).

"narrow AI"—systems designed to perform narrower, more limited problem-solving tasks. We further distinguish in the article between expert systems—systems that utilize AI to simulate human decision-making, reasoning, and judgment, which often require human input—and machine learning, which is a technique whereby machines learn independently without a "human in the loop," and which often requires much greater volumes of data.[6] We recognize that in excavating the role of AI in US intelligence processes, definitions are often used interchangeably by the community. At various points in the article, we attempt to clarify the type of technology under consideration at given time periods and thus illuminate how the technology and its use in intelligence processes have evolved.

We make three arguments that underpin the logic and structure of the article.

One: from the outset, the US intelligence community realized that it cannot develop AI projects strictly in-house, in the same way that it might develop say a listening device or secret camera. It simply does not possess the expertise. We argue that partnerships with the tech sector on AI are an important approach. Intelligence leaders in Washington have acknowledged this for decades. Problematically, as they know only too well, drawing upon outside know-how brings unexpected challenges and can be like opening Pandora's box. The US tech industry is diverse and diffused, located not only in Silicon Valley but also in the Southwest, East Coast, and offices around the world. It is hard to locate on a traditional political spectrum of left and right: the STEM innovators that pull America's twenty-first century economic wagon include a mixture of idealistic dreamers, progressives, "greed-is-good" capitalists, and techno-libertarians who hold an anti-government ethos and are fearful of the surveillance state. Working with such a diverse bunch of ideologies and interests, across national boundaries, makes it hard to get everyone moving in the same direction. As other nations grapple with the global security implications of AI, the lessons learned from Washington's collaboration and contestation with the tech sector are worth noting.

In particular, there are implications for secrecy since some expert collaborators have different belief systems from traditional career intelligence officers. This is not to say that every tech partner is a potential leaker, whistleblower, or traitor: Clearly, there are thousands of tech collaborators whose loyalty to the community and to the nation supersedes personal beliefs and political preferences. Rather, it is about recognizing the potential for cultural tension within the AI ecosystem. In making this point, we continue a conversation initiated by a 2018 article in *Political Studies*, which posits that official secrecy has the potential to be eroded by an influx of technical specialists into the national security space who, ideologically, share similarities with anti-statist techno-libertarians like John Perry Barlow (Aldrich and Moran 2018). Put simply, we see this development as a necessary step for the community, but we also see it as fraught with risk.

Our second argument is that AI is steadily impacting the intelligence cycle—the process of identifying requirements, collecting raw information, processing and analyzing that material, and curating finished intelligence for policymakers and military commanders in the service of national security decision-making.[7] This argument has salience for how intelligence agencies operate around the world and for understanding the changing role of intelligence in global security studies. During the 1980s and 1990s, intelligence professionals were narrowly interested in the data mining and data processing advantages of AI, namely the ability of computers to search through vast troves of raw data, from multiple sources, and transform it into usable information for human analysts. This was reflected in the ECHELON program, an automated global surveillance system involving the Five Eyes intelligence partners, which used content-sensitive dictionaries of keywords and phrases to comb through intercepted satellite communications data for relevant information (Campbell 2000; Aid 2009). The focus of AI projects was directed at trying to assist analysts who found themselves saddled by more useful data than they could ever examine. Today, leveraging the power of AI to help analysts to overcome "data smog"—to find needles in a haystack—remains at the forefront of the community's thinking, aided by graphics for visualization of networks. The data storage giant EMC has estimated that the volume of data in the world doubles every 2 years, with information on the Internet doubling every 90 days. Thus, in the next 2 years, more data will be generated than over the entire period of human history. For agencies, unless solutions can be found, this has the potential to render the global security environment more opaque than knowable. With a lot of data unstructured and located across unintegrated databases, there is hope that machine learning will be able to take some of this

6 For informative recent analysis on the differences between expert systems and machine learning, see Weindling (2022).

7 Our understanding of the intelligence cycle is informed by Pythian (2008). Specifically, we adopt the classic and most widely accepted definition of the cycle as a five-stage process consisting of planning and direction; collection; processing; analysis; and dissemination.

processing strain from human analysts—and even discover things the human brain might miss (Qiu et al. 2016).

However, processing is no longer the only stage of the cycle that the community is hoping to exploit AI. The pursuit of advanced AI systems by rival powers in the international system is creating new intelligence requirements. In this context, understanding how adversaries are developing and deploying AI is becoming central to the work of agencies as the technology itself evolves. There is hope that AI will be able to automate and enhance certain collection tasks, while some professionals are championing the analytical benefits. In terms of disseminating finished intelligence to policymakers, the final stage of the cycle, there is confidence that AI will help to break down structural pathologies, especially stovepipes that impede efficient dissemination, to ensure that bureaucratic turf wars and politics do not prevent the right information from getting into the right hands at the right time. Outside of the cycle, the community is trying to develop AI (including self-learning, adaptive, and automated systems) that protects government networks from cyberattacks. This portends a wider counterintelligence role for AI, where adversarial automated and self-learning systems are used to corrupt, poison, or interfere with data and affect the integrity of the cycle as a whole.[8]

Our final argument is that the community will not be able to exploit AI to its full potential. This was a theme that surfaced during the confirmation hearings of William Burns as President Joe Biden's CIA Director. In his testimony, in February 2021, Burns highlighted that US agencies had to contend with laws governing the collection and use of private data that do not exist in authoritarian countries. These include laws not only made on Capitol Hill but also in the legislatures of countries and power blocs that Washington has security relations with, like the European Union (EU). Another limiting factor is the role of tech collaborators who will not passively allow government agencies to weaponize their technology in ways that do not align with their own interests and ideology. We have already seen this in the clashes between Apple and the Federal Bureau of Investigation (FBI) over encryption and the Bureau's right of access to secured communications stored on the iPhones of suspected terrorists. In each case, Apple argued that it had a "responsibility to protect your data and your privacy" (Vella 2016), indicating a clear tension between the security objectives of the federal government and the privacy standards of the tech sector.

8 For an analysis of the utility of machine learning in data poisoning, see Koh, Steinhardt and Liang (2022).

For these reasons, we conclude that it is premature to suggest that AI will revolutionize intelligence affairs.

## From Bletchley Park to Silicon Valley

Interest in AI among US intelligence actors long predates the twenty-first century. This is not surprising when we consider that much of the early development and philosophy of AI came from Second-World War codebreakers. The idea of AI is widely credited to a 1950 paper by Alan Turing, the Cambridge mathematician who led the team at Bletchley Park that broke the German Enigma code. In the 1950s and 1960s, Bletchley alumnus Donald Michie played a critical role in the development of AI at the University of Edinburgh. At the time, his ideas went beyond the ability of computers to implement them, so to make his point about AI's potential, he developed MENACE, a machine built from 304 matchboxes capable of learning to play the perfect game of noughts and crosses (GCHQ 2021, 23).

In the 1970s, there was something of an AI winter as government departments and private investors cut research funding, having grown tired of waiting for practical AI applications (McKinsey 2017, 9). The slow progress led computer scientists to joke that "If it works, it's not AI" (Archive2 1987). By the early 1980s, however, AI research took an important step forward, with the creation of "expert systems"—software that could replicate human decision-making and judgment (Archive2 1987). Around the same time, the first computer-controlled autonomous vehicles were created (Archive2 1987). With these advances, the way US intelligence looked at AI changed from passive curiosity to active exploration.

The driving force behind the community's first serious investments in AI was John McMahon, who became deputy director of Central Intelligence (DDCI) in April 1982. In a 30-year career at the CIA, McMahon held almost every major managerial position (Archive3). Technology was close to his heart and to the jobs he performed. From 1960 to 1965, he served as executive officer of the Development Projects Division in the Directorate for Plans, which oversaw the U-2 spy plane program. Between 1965 and 1970, he was deputy director of the Office of Special Projects. In 1970, he was appointed director of the Office of Electronic Intelligence, and in 1973, he became chief of the Office of Technical Services, which supervised the design and manufacture of specialized intelligence equipment, hence its reputation as the CIA's Q-branch (Archive3). Because of his broad exposure to the "wizards of Langley," he was ahead of his time in realizing that, with more data,

improved algorithms, and more processing power, AI could transform the spy business.

McMahon was instrumental in overhauling how the community thought about AI. Soon after becoming DDCI, he instructed the Intelligence R&D Council to start a dialogue with possible tech partners, emphasizing that "AI hold[s] great promise and can be of tremendous value to the intelligence community" (Archive4 1982). Richard DeLauer, chairman of the council, agreed: "We must redouble our efforts to take fullest advantage of this technology" (Archive5 1982). In December 1982, at CIA headquarters in Langley, McMahon organized the first in what would become an annual AI symposium, featuring some 500 participants from government, industry, and academia. As well as presentations, the symposium included a vendor show where companies exhibited their AI products. In his keynote, he enthused: "As one who devoted his career to matters of intelligence, I never thought I would see the day where I could proudly announce that we are actively pursuing the creation of artificial intelligence" (Archive6 1983).

A few months later, he established an AI steering group of the Intelligence R&D Council plus several inter-agency committees (Archive6 1983). He requested briefings from the Pentagon on what the military was doing with AI, so that "I can size what the intelligence community ought to be pursuing, watching or piggybacking" (Archive7). By mid-decade, he had rolled out a community-wide training program to "acquaint upper and mid-level management with AI principles, procedures and utility" (Archive8 1983). Ignoring public condemnation about "spies on campus," triggered by press revelations that the CIA had snooped on faculty and placed recruiters in classrooms, he arranged an officer-in-residence program for senior CIA staff to study AI at Carnegie-Mellon University. In return, the University received an annual grant of $75,000 in "research funds" from the Internal Revenue Service (Archive9 1986; Archive10 1987).

With memories of how contractors had accelerated the U2 program when CIA expertise was insufficient, McMahon realized that the community could not develop AI on its own. It needed know-how that could only come from outside, specifically from the tech industry and academia. This message dominated his keynote at the second AI symposium, held at the Defense Intelligence Agency (DIA) headquarters in December 1983, where he stressed that AI was a "multidisciplinary field of endeavour" that required the input of various stakeholders to determine "how we go about transferring it into our line of work" (Archive7 1983).

Under his guidance, the community established partnerships with tech companies from the San Francisco Bay area, the AI capital of the world, including Teknowledge, Intellicorp, and Logicon (Archive2 1987). Relationships were forged beyond Silicon Valley. In March 1987, the Senior Vice President of Texas Instruments gushed to acting CIA director Robert Gates that his company was delighted to "reflect your needs" (Archive11 1987). Investments were made in AI start-ups, and intelligence veterans were encouraged to serve on company boards and nurture personal relationships with senior technology bosses. By the summer of 1984, the AI steering group reported that these contractors had "started to invest in the necessary computer infrastructure and [had] begun to understand our unique needs" (Archive12 1984). Later, as President Ronald Reagan looked to bring the Soviet economy to the brink of collapse by massively increasing US defense spending, the community and its collaborators received funds via the Strategic Computing Initiative, a $600 million war chest for advanced computer hardware and AI. With the geopolitics of the "second cold war" driving technological innovation, the Army developed a self-driving tank, while the Air Force designed an "electronic co-pilot" that communicated in English and assisted with navigation (Archive2 1987).

For the community, building links with technical specialists is vital in helping to develop AI for national security purposes. However, as readers familiar with debates about the "Cultural Cold War" will know—specifically, the often tricky relationships forged by the CIA with artists, musicians, and writers—overt and covert alliances between state and private actors ("state-private networks") are rarely without their challenges (Laville and Wilford 2005). In the case of government relationships with the tech industry, there is the problem that some collaborators hold different ideas about secrecy, security, and the state.

An early illustration of this issue came in the shape of a certain Pierre Blais, a Logicon employee who was contracted to the CIA from 1980 to 1986. Blais's background contained a host of red flags that ordinarily would have made him unsuited for intelligence work. As a teenager, he had been a juvenile delinquent who rode with a motorcycle gang. In 1964, he was arrested for theft; 7 years later, he was arrested again for drug dealing. After college, he joined a religious cult that practiced "weird apocalyptic nationalism" (Archive2 1987). Ideologically, he subscribed to technolibertarianism, which had taken root with the Internet's early hacker community. Now synonymous with figures like Wikileaks founder Julian Assange, counterculture gadfly

Timothy Leary, and activist web guru John Perry Barlow, technolibertarianism is a philosophy that is agnostic to the state, abhors regulation, and deplores the weaponization of technology for national security. Its most famous articulation is found in the opening lines of Barlow's 1996 *Declaration of the Independence of Cyberspace*: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" (Barlow 1996). For Barlow, the unassailable march of technology will eventually destroy the state, in a process described as the United States' "technological Manifest Destiny."

Despite Blais's beliefs and chequered background, he was recruited by the CIA for his computer skills. A brilliant mathematics graduate, his knowledge of AI was dizzying, eclipsing anything that the agency had on its payroll at that time. He joined a team contracted to build a computer system, SAFE, that could automatically pool messages from all over the world, read them, clean them, reformat them, and then dispatch them to the appropriate desks inside CIA headquarters (Archive2 1987).

Blais initially enjoyed the job, which was stimulating and paid well. The longer he stayed, however, the more the work jarred with his ideology. In 1986, having concluded that AI was being developed to create macabre surveillance tech, he quit and took his grievances to the press. He compared his time in Langley to that of an unquestioning German scientist in the Third Reich, alleging that the agency had him working on "immoral, 1984 stuff" (Archive2 1987). Describing the circumstances behind his resignation, he claimed that his bosses had given him a two-inch-thick proposal to develop a computer program that could read a person's mind by analyzing their every blink and twitch. Although his superiors said, "Don't worry, it's just for using on the Russians, in things like arms negotiations," Blais feared that such technology could easily be turned against American citizens (Archive2 1987). After leaving the CIA, he relocated to Santa Cruz, California, where, living in a house of hackers and tech evangelists, he tried to design what he called "AI for masses," a program designed not for CIA mainframes but for personal computers so that citizens can reverse the gaze and spy on the government.

Blais is not an isolated case. A more serious example of someone with techno-libertarian beliefs turning against the community is CIA hacker Joshua Schulte, who (as of this writing) stands accused of stealing 34 terabytes of data—some 2-billion pages of material—and passing it to WikiLeaks. FBI records featured in his prosecution reveal a long history of anti-social and abusive behavior. In his youth, allegedly, he was caught drawing swastikas, making inappropriate sexual advances toward female classmates, and discussing child pornography in online chat rooms. Like Blais, he espoused technolibertarianism. At college, while studying for an engineering degree, he regularly blogged about the government infringing on people's rights. Despite these warnings, his technical expertise appealed to the CIA, and he was recruited as a coder in the Operations Support Branch, the agency's secret hacker unit, where he gave himself the nickname "Bad Ass," another red flag. In November 2016, he resigned following a series of workplace disputes and was concerned about government hands on the technology frontier. In March 2017, he was accused of leaking the contents of "Vault 7," a vast collection of offensive cyber tools, including source code, to Wikileaks. It has been described as the largest unauthorized disclosure of classified information in the agency's history (Keefe 2022).

The Blais and Schulte episodes highlight a wicked problem for the community as it looks to take advantage of AI: How to preserve secrecy when there is a possibility, however small, that some of the IT talents holds culturally divergent or even anti-government beliefs? Intelligence leaders find themselves in a catch-22 situation. If they do not employ these people on security grounds, then their AI projects will stall. But, by employing them, they risk laying organizational land mines, in the form of future disgruntled staff, leakers, and whistleblowers. In authoritarian regimes, this is less of an issue because the tech industry and its workforce come under state control. It is hard to say with precision how widespread anti-government thinking is within the US tech sector today, with the dawn of the original internet bubble in the 1990s generally seen as the high point of technolibertarianism. And, of course, just because someone identifies with this philosophy does not automatically mean they will damage the community in the future. An interesting perspective on the ideology of the tech sector was provided in 2015 by Peter Swire, a leading data privacy lawyer who was a member of President Obama's Review Group on Intelligence and Communications Technology, set up in the wake of Edward Snowden's disclosures about mass surveillance. Swire's research suggested a clear cultural divide between Washington and the sector. Strikingly, whereas not one person that he interviewed from the intelligence community called Snowden a whistleblower, more than 90 percent of Silicon Valley employees used the term (Swire 2014). In his memoir, *Playing to the Edge*, former NSA and CIA Director Michael Hayden conceded that he had paid insufficient attention to the ideological persuasions of the tech sector, the result being that he inadvertently let some foxes into the intelligence

hen house (Hayden 2016). Yet, as Hayden admitted, the community cannot maximize the potential of emerging technologies without taking this risk. "This is a team sport," underlined Dawn Meyerriecks, the CIA's top technologist, in a speech in 2019 (Barnett 2019).

## Helping with Data Smog

By the 1980s, agencies recognized that their chief problem was not information scarcity, but information overload. In 1985, Lt. General James Williams, the Director of the DIA, reported that the agency received about 10,000 messages per day for processing, in contrast to 5,000 only a few years before, and analysts were struggling to keep up with the workload (Archive13 1985). This was just the start of the problem. Today, the flow of information reaching the community has been likened to being hit by a fire hose, greatly exceeding the ability of analysts to make sense of it. In 2017, the National Geospatial-Intelligence Agency forecasted that, within 5 years, the torrent of data pouring into the organization from government and commercial satellites, sensors, and drones would increase by a millionfold (Vinci 2020). In early 2021, the ODNI estimated that by the end of the year, through its web-based open sources alone, it will have amassed 3.3 trillion gigabytes of data (Fitzgerald 2021). For intelligence analysts, this mounting barrage of data is too enormous to process without support, and potentially significant things will be missed. To illustrate the point, in 2017, an assault on an Al Qaeda safe house in Afghanistan yielded 40 terabytes of data. For the sake of argument, let us assume that a quarter of that data was in video form: It would take someone 208 days, working 24/7, to review the footage (Washabaugh 2021). Clearly, no analyst has the bandwidth for this.

AI has long been held as a panacea to the problem of data smog. In December 1982, DeLauer declared that "AI is the only technology with the promise of yielding the kinds of information systems needed to process the projected volume of data and present it in a way that is meaningful to and efficient of our human analysts" (Archive5 1982). Early thinking by DeLauer and other bosses focused on how AI could be exploited to do what we might call the dirty work of data mining and data processing. Before finished assessments can be crafted for policymakers, there is a lot of heavy lifting in the shape of data cleaning, sorting, reformatting, labeling, annotating, and pattern recognition. As they saw it, the main advantage of AI was that it could pick up a lot of this vital but burdensome activity and be deployed alongside humans to enhance decision-making. With AI preparing and triaging raw collected data, human analysts would have more time to evaluate material and apply their expertise and problem-solving ability. "AI and expert systems have the potential to permit the agency to leverage its most critical resource—its people," emphasized Edward Maloney, CIA director of Information Technology, in October 1986: "Expert systems will be a significant productivity tool, freeing up personnel currently performing straightforward tasks . . . Not only will we be able to automate many tasks currently requiring an 'expert,' we will be able to ensure consistency, provide backup, and improve the speed of decisionmaking" (Archive14 1986).

In the 1980s and 1990s, efforts to offload mundane processing tasks onto AI were hamstrung by the infancy of the technology. Modest success was achieved in developing speech-to-text transcription as well as automated speaker recognition software capable of identifying human speech in noisy environments (Archive6 1983). The NSA developed a program to help transcribe and translate foreign language materials. This proved invaluable in helping to deal with the mass of intercepted Soviet phone calls that the agency collected during the late Cold War (Anon 2021). Ultimately, however, ambition exceeded what was scientifically possible. Indeed, in Afghanistan during the Bush-era "war on terror," American personnel on the ground relied on native speakers rather than automated translations (Anon 2021).

In the twenty-first century, computational tools powered by machine learning are having greater success in automating basic tasks. Consequently, it is expected that human analysts will have more bandwidth for strategic work. One study has suggested that AI is now saving a typical all-source intelligence analyst more than 45 working days a year (Fitzgerald 2021). To quote a recent article, AI is increasingly skilled at carrying out "thinking fast" assignments—processing tasks that human analysts perform intuitively and quickly, like spotting and recognizing a Russian Tu-95 bomber from a satellite image (Hampel-Arias and Meyers 2021). Where AI struggles are the "thinking slow" part of the intelligence cycle—commonly understood as analysis. Analysis requires intuition and deliberative thinking. It involves using this knowledge to turn raw data into predictions and policy options. For example, a "thinking slow" assignment would be divining from the same satellite image where the bomber took off from, where it is heading, and what it is doing in the sky.

Considerable progress has been made in terms of the think-fast ability of AI to mine massive data sets to detect keywords, phrases, and objects of interest. Housed within the CIA's Directorate for Digital Innovation, the Open Source Enterprise uses AI to comb through global news articles and public broadcasts, in near real time, in

search of flagged material of security interest. "Imagine that your job is to read every newspaper in the world, in every language, watch every television show," claimed Dean Souleles, the chief technology adviser to the ODNI in 2020. "That's the job of the Open Source Enterprise, and they are now using technology tools and tradecraft to keep pace" (Tucker 2015). At NSA, machine-assisted fact-checking is helping to reduce the time that analysts spend looking for deepfake internet content, by cross-referencing against trusted sources and tracking bots that infiltrate social networks to mimic real users and spread disinformation.

One of the CIA's technological successes in this area has been its work with the software company Palantir Technologies, named after the all-powerful, far-seeing crystal balls from J.R.R. Tolkien's *The Lord of the Rings*. According to author Mark Bowden, Palantir software was instrumental in the hunt for Osama bin Laden, helping to find tell-tale words about the terrorist's location, which it put into maps, histograms, and link charts, from a marshland of unstructured message traffic, network data, telephony, and stolen documents (Bowden 2012). Corroborating this view, former CIA director and commander of NATO forces in Afghanistan General David Petreaus has described Palantir's machine learning algorithm as a "better mousetrap when a better mousetrap was needed" (Greenberg and Mac 2013). As Andy Greenberg and Ryan Mac explain, Palantir has become a highly useful data mining and analytical tool: "Palantir has become the go-to company for mining massive data sets for intelligence and law enforcement applications, with a slick software interface and coders who parachute into clients' headquarters to customize its programs" (Greenberg and Mac 2013).

## Changes in the Intelligence Cycle and their Implications for Global Security

AI presents possibilities and pitfalls for US intelligence agencies beyond data processing. As other nations, especially enemies, develop their own AI capabilities, US policymakers will need to adjust their intelligence requirements, which provide direction to intelligence managers on what to collect and analyze. Of particular importance to policymakers in Washington will be the types of AI being developed by adversaries, their level of complexity, their weaknesses, and the doctrines that govern their use in military-strategic contexts. Building a sophisticated picture of these issues will not be easy, especially when it comes to closed societies like China. The US intelligence community continues to be hamstrung by a dearth of trained Mandarin speakers (Hamilton 2022), while the political leadership in Beijing is notorious for cracking down on anything that smacks of foreign espionage in the country (Dorfman 2021). Moreover, as national security practitioner Brian Katz argues, the rapid rate of innovation in the AI field makes "prioritization difficult and can quickly render well-laid planning obsolete" (Katz 2020).

China has already modified its own intelligence requirements to acknowledge the growing importance of AI. There have been well-documented efforts by Beijing to place spies in US universities to steal intellectual property relating to all types of AI (both techniques and technologies). China is determined to learn more about US AI processes and thinking, especially with respect to deep learning, neural networks, responsible AI, and pathways to AGI. To support its own AI systems, Beijing is desperate for access to advanced microchips produced by the United States and its Asian allies, Taiwan and South Korea.[9] Campaigns of Chinese cyber espionage have targeted developmental processes in US tech companies that have connections with the national security establishment. As one report in the *National Review* notes, "Major lines of effort in Beijing's foreign acquisition strategy include 'talent programs,' exploitation of American universities, hacking and theft, and investment in American firms to acquire American technology" (Blumenthal and Zhang 2021). These surreptitious activities are designed not only to accelerate China's proficiency with emerging technologies, but also to provide Beijing with a window into the US AI ecosystem and its fragilities.

Intelligence professionals are predicting a significant role for AI at the collection stage of the intelligence cycle. Katz anticipates that AI will be able to help in automating the planning, scheduling, and tasking of collection efforts based on knowing the requirements and the type of target (Katz 2020). He envisages a future where AI will forecast collection tasks, select the most suitable asset (human or virtual) for the objective, and schedule collection missions based on task frequency and scope. One day, he even thinks that AI could assist human collectors in spotting, assessing, and recruiting human intelligence assets (Katz 2020).

What about analysis? In the past, as we have seen, the main value of AI for human analysts was the prospect of offloading tedious tasks onto machines. Today, analysts are now thinking more ambitiously about a new form of collective intelligence, with computers and people working in tandem to take advantage of psychology's ever-better grasp of how learning is achieved, the objective

9 For an analysis of China's AI priorities, see Hannas et al. (2022).

being that AI will make people smarter just as people make AI smarter. Out of this partnership, it is hoped that AI will in time help analysts to overcome some of the cognitive biases that have contributed to historic intelligence failures.[10] For example, there is the potential for AI to identify if an assessment has been guilty of "under-warning" (i.e., neglecting vital information) or the opposite problem, "over-warning" (i.e., putting too much emphasis on certain information and thus issuing false alarms), sometimes referred to as cry wolf syndrome. There is also the potential for AI to detect if analysts have lost their objectivity by telling policymakers only what they want to hear or, alternatively, by provoking policymakers by telling them only what they do not want to hear.[11]

There is growing optimism within the community that one day AI will be able to turn the digital trail that humans leave behind into a crystal ball into the future. This has long been an aspiration. In 1983, McMahon hoped that AI might be used to provide expert medical diagnoses of foreign leaders (Archive6 1983). A year later, he spoke about "sophisticated simulation and modelling techniques increasing our ability to predict alternative outcomes of future events" (Archive15 1984). Today, AI-based anticipatory intelligence capability is moving forward. In 2011, the Intelligence Advanced Research Projects Agency established Open Source Indicators, a program designed to forecast global societal events—from mob violence to humanitarian crises—through the automated examination of publicly available data, including social media, news articles, and weather reports. In 2012, Virginia Tech researchers used this program to predict two cases of civil unrest, in Mexico and Paraguay, even getting the date and timing of the protests correct in both instances (Tucker 2015). At the NSA, AI screens for anomalies in broader patterns of web traffic that could portend an impending hostile act (Fitzgerald 2021). Andrew Hallman, a former head of CIA Digital Innovation, has controversially suggested that social media is such a good barometer of a population's temperature that, with AI-powered sentiment and predictive analysis, the community is unlikely to be blindsided by events like the Arab Spring again (Fitzgerald 2021). We are skeptical about this. Before the Arab Spring, agencies were determined to forecast the spatial and temporal dimensions of conflict in the Middle East and used social media extensively for this purpose. Yet, they still failed to anticipate it. Also, as Jinghan Zeng has written, AI is just as likely to be used by states to suppress uprisings as predict them (Zeng 2020).

AI is set to impact the final, dissemination stage of the cycle. One area seems ripe for the application of AI: the age-old problem of stovepiping. This occurs when intelligence does not reach its intended recipient because of political pressures, bureaucratic red tape, or plain human error. Famous instances of stovepiping include the strategic surprises of Pearl Harbor and 9/11. If AI is deployed at all stages of the cycle, then the cycle itself could be automated, with machines determining requirements, identifying targets, collecting data, and analyzing it, before disseminating finished product to decision-makers free of human intervention and organizational blockages. In situations where rapid decisions need to be taken, enhancing the speed of the cycle could prove invaluable. Of course, there will need to be efforts to verify the efficacy of automated processes, eliminate bias, and check for corruption in the cycle. This is reflected in an emerging debate over whether a "human in the loop" will be needed, desirable, or even possible as AI technology evolves (Mellamphy 2021). The notion that AI could be harnessed to overcome stovepiping is not simply a theoretical proposition, only to be realized long into the future. In 2018, the Defense Advanced Research Projects Agency (DARPA) reported that it had 20 projects on the books that aim to enhance the contextual reasoning of AI (the ability to learn from its own environment) in ways that break down what is known by the community as the stovepiping "Wall" (DARPA 2018).

Outside of the cycle, AI is being developed by US intelligence for cyber offense and defense. In recent years, offensive cyber operations and the use of AI in information operations by America's enemies have grown in scale and sophistication. Since its illegal annexation of Crimea in 2014 through to its ongoing invasion of Ukraine, Russia has waged a sustained disinformation campaign designed to justify its military aggressions, targeting its own population, its neighbors, and the international community at large. Then, of course, there was the work of Russian intelligence in spreading dangerous myths on social media in a bid to influence the result of the 2016 US presidential election. The impact of this weaponization of AI by Russia—together with conventional cyberattacks, targeting Democrat party officials through hack-and-leak operations—is hotly

10 Ideas about the fusion between computers and people at the analytical stage feature in a 6-week course at MIT entitled "Artificial Intelligence: Implications for Business Strategy." We are grateful to Dr James Lockhart (Rabdan Academy) for pointing this out to us.

11 For a fascinating discussion of the causes of intelligence failure and, by extension, how AI could help to minimize or even negate the subjectivity of human cognitive processes, see Priess (2021).

contested. While some like Katarina Kertysova suggest that it was instrumental in swaying the voting decisions of many American citizens in 2016, others like Thomas Rid are more skeptical (Kertysova 2018; Rid 2020).

In response to efforts by hostile powers to corrupt political processes, the US intelligence community is investing heavily in AI projects designed to prevent intrusions that target officials and agencies. As the director of the Joint AI Center at the Pentagon recently attested, this has entailed a mind shift in the community's approach to network security: "Our networks are weapons, and, so, we must treat them like weapons. We must plan to protect them, make them resilient because everything that we're going to do in an artificial intelligence or data-driven way will depend on the security [of] those networks" (Vergun 2021). One project is CylancePROTECT, which is used by the CIA to prevent malware and email phishing scams from compromising its operations. According to one expert, the machine learning model behind the software was trained on millions of emails until it could distinguish between safe forms of digital communication and suspicious ones that had to be neutralized (Roth 2019). New capabilities like this speak not only to the role of private actors in the security space, but the "cyber-fication" of spying—the reliance on computers in intelligence work—a process that has implications for intelligence agencies around the world.

## Revolution?

In 2016, the US Department of Defense Office of Net Assessment concluded that the strategic advantage offered by AI will soon eclipse the advantage held by the Allies during the Second World War after they had broken the German Enigma and Japanese Purple codes (DoD 2016). We are not convinced by this. Data is the lifeblood of AI-led intelligence, but it is not certain that agencies will be able to access what they need. There are laws that govern how agencies can collect data and how long they can retain it for analytical purposes. Following Snowden, there is now greater congressional scrutiny of the use of legislation like Section 702 of the US Foreign Intelligence Surveillance Act (FISA), which is believed to have resulted in the "incidental" collection of millions of Americans' communications between 2008 and 2013. Importantly, regulations exist not only internally in the United States, but externally, on the statute books of friends and allies with whom Washington has security relations. The EU has exacting rules on what data US agencies can request on European citizens on national security grounds. As Theodore Christakis and Kenneth Propp have enunciated, "EU law provides no national security exemption that may be invoked on behalf of third-state intelligence services" (Christakis and Propp 2021). Both the European Court of Justice (CJEU) and the European Data Protection Board can impose heavy fines on companies that transfer data to the United States in instances where it is found that the EU's restrictive surveillance standards have not been met (Christakis and Propp 2021).

This is not to say that agencies will not look to change or circumvent the rules. Agencies will fight for there to be exemptions for security analytics. In early 2022, senators Ron Wyden and Martin Heinrich—both of whom sit on the Senate Intelligence Committee—alleged that the CIA was bypassing the judicial and congressional oversight that comes with FISA by carrying out bulk collection under the authority of the Reagan-era Executive Order 12,333 (Meyer 2022). Even in the EU, where the rules on data collection, retention, and protection are much stricter than in the United States, there has been pushback by individual member states on security grounds. This has manifested most obviously in the stalled negotiations that have accompanied the revision and replacement of the EU e-privacy directive. France insisted that it would not support the regulation unless it contained a broad security clause that permits data collection and retention by intelligence agencies. As a result, discussions were deadlocked for 5 years. France's obstinance on this issue mirrored its earlier efforts to ensure that CJEU rulings and GDPR did not prevent data retention by law enforcement (Christakis and Propp 2021).

Nevertheless, the overall trajectory of the regulatory landscape is one that will likely see more, not less, control over how agencies can exploit big data and AI for national security purposes. This will, of course, depend on the purpose for which the data is sought and how quickly it is required. At the time of writing, the EU is debating its proposal for an "Artificial Intelligence Act" (EU 2021). Underpinning the proposal is an ethical, human-centric, and risk-based approach dictating that stricter rules will be applied depending on the intended purpose of the AI system. The greater the risk to civil liberties, the greater the control. States caught violating the rules will be fined up to 6 percent of global turnover. As the first serious attempt to regulate AI, the EU's proposal is attracting global interest (Engler 2022). In the United States, there are signs that lawmakers are open to pursuing a similar risk-based approach. However, unlike Brussels, which is aiming for a comprehensive regulatory framework for AI, Washington favors regulatory guidelines on an agency-by-agency basis. Important in this context is the final report of the National Security Commission on AI, submitted to Congress in March 2021. In it, the commissioners forecast the likely direction of travel on regulation

by recommending that "the government take certain domestic actions to protect privacy, civil rights, and civil liberties in its AI deployment" (National Security Commission on AI 2021). The US Government Accountability Office has also joined the chorus of voices calling for regulation, arguing that the principles of responsibility and accountability should be embedded in the "design, development, deployment, and continuous monitoring of AI systems" (Sussman, McKenney and Wolfington 2021).

Whether in the form of federal regulation (not ruled out, but unlikely) or a smorgasbord of soft laws, ethical frameworks, and voluntary guidelines, it is clear in general terms that US agencies will face significant hurdles in being able to maximize the value of AI technologies (Villasenor 2020). On October 4, 2022, the Biden White House looked to demonstrate its commitment to "responsible" AI by publishing a (non-binding) blueprint for an AI Bill of Rights. Put together over a period of 12 months in consultation with multiple government departments, civil society groups, and tech companies, the document highlighted that the use of AI "must not come at the price of civil rights or democratic values" (White House 2022). To this end, it included guidelines on how to safeguard data, reduce the risk of bias, and limit the use of surveillance, although tellingly its recommendations about surveillance related to the commercial rather than the national security sector (Morrison 2022). There are practical impediments too, like data storage. As Meyerriecks has observed, "We can't just keep data forever and ever, kind of filling up our servers, right? So there's lots of culling that goes on pretty much continuously and grooming" (Swisher 2021).

Then, there are the principles of tech collaborators to negotiate. A good example of this difficult negotiation came in 2018 when over 3,000 Google employees signed an open letter calling for the company not to renew a contract with the Pentagon for Project Maven, an AI program that analyzed drone surveillance footage and identified suspected terrorists for targeting (Vogel et al. 2021, 827). While Maven liberated analysts from hours of tedious sifting through video imagery, Google employees worried that it might be used to automatically launch drone strikes without a human operator. Following the petition, which saw twelve engineers resign in protest, Google CEO Sundar Pichai announced that he would walk away from the contract renewal and published a new code of ethics stipulating that the company will not design AI "whose principal purpose or implementation is to cause or directly facilitate injury to people" (Google 2018). The rank-and-file workers of the tech sector represent a powerful line of defense against overreach by agencies in their utilization of AI for intelligence purposes.

## Conclusion

This article has sought to shine a light on how the US intelligence community is engaging with AI. The literature on AI and global security has tended to focus on the consequences of AI for the nature and character of war and how it is being harnessed by leading powers like the United States, Russia, and China to give them a competitive edge in military terms. Only recently have scholars started to ponder the competitive advantages of AI in the intelligence domain. Contributing to this new area of inquiry, our analysis has shown that agencies have been interested in AI since at least the 1980s. This is important to acknowledge because these historical interactions and experiences have shaped contemporary thinking within the US national security apparatus. The momentum for this early engagement was provided by senior leaders at the CIA, like DDCI John McMahon, who realized that intelligence work requires tech wizards as well as James Bonds and Jack Ryans. As a result, the community is now enjoying the benefits of this head start, with a knowledge base to draw on and clear ideas about how AI can be harnessed to protect national security. Moreover, first-mover advantage has ensured that the United States has created precedents that other AI powers need to comply with, negotiate or resist.

The US intelligence community has long recognized the importance of collaborating with outside specialists on AI. As a result, it is now deeply embedded in the latest research projects coming out of the tech sector. It has been learned that working hand in glove with STEM innovators is not straightforward. There is an uneasy footing between the community and the sector. As the cases of Blais and Schulte illustrate, there are risks attached to asking some collaborators to do jobs that are alien to their core values, especially when it comes to protecting classified information. Quoting Winston Churchill, in November 2021 Britain's SIS chief Richard Moore has said that he expects the service's new tech partners to behave just as the Cambridge scientists at Bletchley Park behaved during the Second World War, as "the geese that laid the golden eggs but never cackled" (Moore 2021). The problem with this analogy is that the scientists at Bletchley had a lot in common with their intelligence overlords. They were fighting a common enemy and attended the same schools, universities, and clubs. There was a degree of ideological and political alignment. For all their professional differences, like leopards and ocelots, they were both cats with spots. Can the same be said for the tech partners that agencies are looking to build relationships today? Part of the problem is that the tech sector is made up of so many diverse constituencies: It is hard to

pinpoint an overarching belief system. Ultimately, only time will tell how deeply technolibertarianism is woven into the fabric of the sector and what this means for the development and use of AI in the national security field.

After initially focusing on the data processing advantages of AI, which remain front and center in the community's thinking, attention is now being given to how AI can improve all stages of the intelligence cycle. The cycle has never been a perfect conceptual tool and has long attracted criticism from scholars for failing to precisely capture how intelligence processes work. As Arthur Hulnick wrote in 2006, while almost all intelligence professionals regard it as a "kind of gospel," the cyclical pattern fails to recognize that collection and analysis often work in parallel, not in sequential stages, while the notion that decision-makers patiently wait for the delivery of intelligence before making policy is flawed (Hulnick 2006). It is our view that the cycle will warrant further reconceptualization in the context of emerging technologies. There are observations to be made about the speed of the cycle and whether effective oversight and human control of it is sustainable in the context of the sophisticated automation processes that AI provides and the growing involvement of tech collaborators. The cycle will require rethinking as AI converges with cloud computing, the internet of things, and robotics.

We nevertheless feel that it is too early to proclaim a revolution in intelligence affairs. Just as John Ferris concluded about the so-called "Revolution in Military Affairs"—when he wrote that new concepts like "net-centric warfare," "C4ISR," the "infosphere" and "information operations" had "multiplied American strengths but not reduced American weaknesses"—we believe that while AI is changing many things its power will be limited by human factors (Ferris 2004). Within the agencies, the full potential of AI will be constrained by the humans that express requirements, design technology, and use it. Access to data will be constrained by evolving regulations put forward by a coalition of legislators, tech companies, civil society activists, and overseas partners like the EU. Tech partners will not march in lockstep with agencies if they feel that their ideology or their user privacy is being threatened. Worryingly for agencies, many tech companies are simultaneously invested in democratizing AI technologies as widely as possible, by providing private citizens with "off the shelf" intelligence devices, including AI-driven software for voice and facial recognition. The ability to run agents, build "cover" and carry out clandestine operations will be diminished in a world where cheap surveillance technology is widespread thanks to tech companies realizing Blais's dream of "AI for the masses."

Overall, then, it is too early to claim that we are moving from the era of secret intelligence to smart spying.

## Acknowledgments

This article was made possible by generous support from the Institute of Advanced Study (IAS) at the University of Warwick. The authors are especially indebted to the IAS for hosting Joe Burton as a Fernandes Fellow, which facilitated a 3-month period of research collaboration and writing, free from the daily grind. For shepherding the article into print, the authors are grateful to the journal editors plus production team, so too the peer reviewers for their constructive feedback over several iterations of the piece.

## References

Abbass, Hussein. 2021. "What is Artificial Intelligence?" *IEEE Transactions on Artificial Intelligence* 2 (2): 94–95.

Aid, Matthew. 2009. *Secret Sentry: The Untold History of the National Security Agency*. New York: Bloomsbury.

Aldrich, Richard J., and Christopher R. Moran. 2018. "'Delayed Disclosure': National Security, Whistle-Blowers, and the Nature of Secrecy." *Political Studies* 67 (2): 249–69.

Allen, Greg, and Taniel Chan. 2017. *Artificial Intelligence and National Security*. Cambridge, MA: Harvard Kennedy School.

Andrew, Christopher and David Dilks, eds. 1984. *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*, London: Palgrave.

Anon. 2021. "High Hopes for AI." *Economist*.

Archive1. 1983. "Interrogation of an Alleged CIA Agent." *Studies in Intelligence*, CIA Records Search Tool (hereafter CREST).

Archive2. 1987. "The Divided Mind of Artificial Intelligence." CREST.

Archive3. Date unknown. "An Interview with Former DDCI John McMahon." CREST.

Archive4. 1982. John McMahon to Richard DeLauer. CREST.

Archive5. 1982. Richard DeLauer to John McMahon. CREST.

Archive6. 1983. "John McMahon: Address to the Second Annual Symposium on AI Applications in the Intelligence Community. CIA HQ Auditorium." CREST.

Archive7. 1983. John McMahon to Under-Secretary of Defense for Research Engineering. CREST.

Archive8. 1983. Executive Secretary (AI Steering Group) to Director IC Staff. CREST.

Archive9. 1986. Director of Training and Education to Deputy Director for Administration. CREST.

Archive10. 1987. Edward Maloney to Director of Training and Education. CREST.

Archive11. 1987. George Heilmeier to Robert Gates. CREST.

Archive12. 1984. Chairman (AI Steering Group) to Richard DeLauer. CREST.

Archive13. 1985. Executive Secretary to Deputy Director for Intelligence. CREST.

Archive14. 1986. Edward Maloney. "Conference on Agency Priorities." CREST.

Archive15. 1984. John McMahon to Security Affairs Support Association. CREST.

Ayoub, Kareem, and Kenneth Payne. 2016. "Strategy in the Age of Artificial Intelligence." *Journal of Strategic Studies* 39 (5-6): 793–819.

Baker-Eck, Bianca, Ray Bull, and Dave Walsh. 2020. "Investigative Empathy: A Strength Scale of Empathy Based on European Police Perspectives." *Psychiatry, Psychology and Law* 27 (3): 412–27.

Barlow, John Perry. 1996. "A Declaration of the Indepedence of Cyberspace." Accessed September 7, 2022. https://www.eff.org/cyberspace-independence.

Barnett, Jackson. 2019. "AI is Breathing New Life into the Intelligence Community." *Fed Scoop*. Accessed July 24, 2022. https://www.fedscoop.com/artificial-intelligence-in-the-spying.

Bedan, Matt. 2007. "Echelon's Effects: The Obsolescence of the US Foreign Intelligence Legal Regime." *Federal Communications Law Journal* 59 (2): 425–44.

Blumenthal, Dan, and Linda Zhang. 2021. "China is Stealing Our Technology and Intellectual Property. Congress Must Stop It." *National Review*. Accessed August 1, 2022. https://www.nationalreview.com/2021/06/china-is-stealing-our-technology-and-intellectual-property-congress-must-stop-it.

Bowden, Mark. 2012. *The Finish: The Killing of Osama Bin Laden*. London: Grove Press.

Brantly, Aaron. 2018. "When Everything Becomes Intelligence: Machine Learning and the Connected World." *Intelligence and National Security* 33 (4): 562–73.

Burton, Joe, and Simona Soare. 2019. "Understanding the Strategic Implications of the Weaponization of Artificial Intelligence." *11th International Conference on Cyber Conflict (CyCon)*, Institute of Electrical and Electronics Engineers (900).

Campbell, Duncan. 2000. "Inside Echelon." *Heise Online*. Accessed March 1, 2022. https://www.heise.de/tp/features/Inside-Echelon-3447440.html.

Carpenter, Charli. 2016. "The Future of Global Security Studies." *Journal of Global Security Studies* 1 (1): 92–94.

Crawford, Kate. 2021. *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT: Yale University Press.

Christakis, Theodore, and Kenneth Propp. 2021. "How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—And What It Means for the United States." *Lawfare*. Accessed April 1, 2022. https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states.

DARPA. 2018. "DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies." Accessed July 7, 2022. https://www.darpa.mil/news-events/2018-09-07.

DoD. 2016. "Department of Defense Office of Net Assessment. Summer Study: Artificial Intelligence."

Dorfman, Zach. 2021. "China Used Stolen Data to Expose CIA Operatives in Africa and Europe." *Foreign Policy*. Accessed September 5, 2022. https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/

Engler, Alex. 2022. "The EU AI Act Will Have Global Impact, but a Limited Brussels Effect." *Brookings Report*. Accessed August 15, 2022.

Erbschloe, Michael. 2017. *Threat Level Red: Cybersecurity Research Programs of the US Government*. New York: Auerbach.

Eversden, Andrew. 2020. "CIA Launches First Federal Lab." *C4Isrnet*. Accessed June 1, 2022. https://www.c4isrnet.com/it-networks/2020/09/21/cia-launches-first-federal-lab.

EU. 2021. "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts." COM/2021/206 final, 2021/0106(COD), Brussels.

Ferris, John. 2004. "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence and National Security* 19 (2): 199–225.

Fitzgerald, Ian. 2021. "The Impact of AI on the IC." *Cipher Brief*. Accessed July 21, 2022. https://www.thecipherbrief.com/column_article/the-impact-of-artificial-intelligence-on-the-ic.

GCHQ. 2021. "Pioneering a New National Security: The Ethics of Artificial Intelligence." Accessed May 1, 2022. https://www.gchq.gov.uk/files/GCHQAIPaper.pdf.

Goldfarb, Avi, and Jon Lindsay. 2021/22. "Prediction and Judgement: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46 (3): 7–50.

Google. 2018. "AI at Google: Our Principles." Accessed May 27, 2022. https://www.blog.google/technology/ai/ai-principles.

Greenberg, Andy, and Ryan Mac. 2013. "How a 'Deviant' Philosopher Built Palantir." *Forbes*. Accessed March 25, 2022. https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/?sh=26d3c9477785.

Hambling, David. 2021. "AI is Helping US Air Force to Decide Which Targets to Strike." *New Scientist*. Accessed March 24, 2022. https://www.newscientist.com/article/2291586-ai-is-helping-us-air-force-to-decide-which-targets-to-strike/

Hamilton, Jillian. 2022. "CIA Recruiting Mandarin Speakers While Keeping Eye on Russia." *Clearance Jobs*. Accessed January 3, 2023. https://news.clearancejobs.com/2022/04/20/cia-recruiting-mandarin-speakers-while-maintaining-eye-on-russia/

Hampel-Arias, Zigfried, and John Speed Meyers. 2021. "What Can AI Do and Cannot Do for the Intelligence Community." *Defense One*. Accessed March 5, 2022. https://www.defenseone.com/ideas/2021/01/what-ai-can-and-cannot-do-intelligence-community/171195.

Hannas, William, Huey-Meei Chang, Daniel Chou, and Brian Fleeger. 2022. "China's Advanced AI Research: Monitoring China's Paths to "General" Artificial Intelligence." *Center for Security and Emerging Technology*. Accessed December 22, 2022. https://cset.georgetown.edu/publication/chinas-advanced-ai-research.

Hayden, Michael. 2016. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin

Hulnick, Arthur. 2006. "What's Wrong with the Intelligence Cycle?" *Intelligence and National Security* 21 (6): 959–79.

Johnson, James. 2021. "Inadvertent Escalation in the Age of Intelligence Machines: A New Model for Nuclear Risk in the

Digital Age." *European Journal of International Security* 7 (3): 337–59.

Kania, Elsa. 2021. "Artificial Intelligence in China's Revolution in Military Affairs." *Journal of Strategic Studies* 44 (4): 515–42

Katz, Brian. 2020. "The Collection Edge Harnessing Emerging Technologies for Intelligence Collection." *CSIS*. Accessed July 22, 2022. https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection public/publication/20713_Katz_CollectionEdge_v4_WEB%20FINAL.pdf.

Keefe, Patrick. 2022. "The Surreal Case of a CIA Hacker's Revenge." *New Yorker*. Accessed September 7, 2022. https://www.newyorker.com/magazine/2022/06/13/the-surreal-case-of-a-cia-hackers-revenge.

Kertysova, Katarina. 2018. "Artificial Intelligence and Disinformation." *Security and Human Rights* 29 (1-4): 55–81

Knowles, Tom. 2021. "Microsoft Boss Warns AI May Mean Orwell's 1984 by 2024." *Times*. Accessed June 11, 2022. https://www.thetimes.co.uk/article/microsoft-boss-warns-ai-may-mean-orwells-1984-by-2024-96hnlc9p8.

Koh, Pang Wei, Jacob Steinhardt, and Percy Liang. 2022. "Stronger Data Poisoning Attacks Break Data Sanitization Defenses." *Machine Learning* 111 (3): 1–47.

Laville, Helen and Hugh Wilford. 2005. Eds. *The US Government, Citizen Groups, and the Cold War: The State-Private Network*. London: Routledge.

Marks, Robert. 2020. *The Case for Killer Robots: Why America's Military Needs to Continue Development of Lethal AI*. Seattle, WA: Discovery Institute Press.

McAllister, Amanda. 2017. "Stranger than Fiction: the Rise of AI Interrogation in the Dawn of Autonomous Robots and the Need for an Additional Protocol to the UN Convention against Torture." *Minnesota Law Review* 180: 2527–73.

McKinsey. 2017. "Artificial Intelligence: The Next Digital Frontier?" Discussion Paper, June 2017. Accessed March 1, 2022. https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx.

Margulies, Peter. 2016. "Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights." *Florida Law Review* 68 (4): 1045–117.

Mellamphy, Nandita Biswas. 2021. "Humans 'in the Loop'?: Human-centrism, Posthumanism, and AI." *Nature and Culture* 16 (1): 11–27.

Meyer, David. 2022. "The CIA Has Been Conducting Mass Surveillance in the US with Minimal Oversight." *Fortune*. Accessed October 2, 2022. https://fortune.com/2022/02/11/cia-mass-surveillance-wyden-privacy-shield-meta.

Moore, Richard. 2021. "Human Intelligence in the Digital Age." *IISS*. Accessed March 29, 2022. https://www.iiss.org/events/2021/11/human-intelligence-digital-age.

Morgan, Forest E., Benjamin, Boudreaux, Andrew J., Lohn, Mark, Ashby, Christian, Curriden, Kelly, Klima, Derek, and Grossman. 2020. *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica, CA: RAND

Morrison, Ryan. 2022. "US Takes First Step towards AI Regulation with 'Bill of Rights' Blueprint." *Tech Monitor*. Accessed November 5, 2022. https://techmonitor.ai/leadership/governance/us-ai-regulation-bill-of-rights.

National Security Commission on Artificial Intelligence. 2021. "Final Report." Accessed December 20, 2022. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

ODNI. 2013. "The Aim Initiative: A Strategy for Augmenting Intelligence Using Machines." Accessed March 1, 2022. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

Payne, Kenneth. 2021. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst.

Priess, David. 2021. "Afghanistan, Policy Choices, and Claims of Intelligence Failure." *Lawfare*. Accessed August 23, 2022. https://www.lawfareblog.com/afghanistan-policy-choices-and-claims-intelligence-failure.

Pythian, Mark. Ed. 2008. *Understanding the Intelligence Cycle*. London: Routledge.

Qiu, Junfei, Guoro Ding, Yuhua Xu, and Shuo Feng. 2016. "A Survey of Machine Learning for Big Data Processing." *EURASIP Journal of Advances in Signals Processing* 2016: 67. https://doi.org/10.1186/s13634-016-0355-x.

Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.

Reinert, John. 2013. "In-Q-Tel: The Central Intelligence Agency as Venture Capitalist." *Northwestern Journal of International Law and Business* 33 (3): 677–709.

Roth, Marcus. 2019. "Artificial Intelligence at CIA." *Emerj*. Accessed April 2, 2022. https://emerj.com/ai-sector-overviews/artificial-intelligence-at-the-cia-current-applications.

Roumate, Fatima. 2021. "Malicious Use of Artificial Intelligence, New Challenges for Diplomacy and International Psychological Security." In *Artificial Intelligence and Digital Diplomacy: Challenges and Opportunities*, edited by Fatima Roumate, 97–113. Cham: Springer, https://doi.org/10.1007/978-3-030-68647-5_8.

Sussman, Heather, Ryan McKenney, and Alyssa Wolfington. 2021. "US Artificial Intelligence Regulation Takes Shape." *Orrick*. Accessed January 4, 2022. https://www.orrick.com/en/Insights/2021/11/US-Artificial-Intelligence-Regulation-Takes-Shape. For US approach to AI see also: https://www.state.gov/artificial-intelligence.

Swire, Peter. 2014. "Why Tech Companies and the NSA Are Split about Snowden." *Washington Post*. Accessed January 26, 2022. https://www.washingtonpost.com/opinions/why-tech-companies-and-the-nsa-are-split-about-snowden/2014/01/29/e322c746-83ab-11e3-9dd4-e7278db80d86_story.html.

Swisher, Kara. 2021. "CIA's Top Technologist is Uncomfortable with Facebook." *New York Times*. Accessed March 2, 2022. https://www.nytimes.com/2021/04/26/opinion/sway-kara-swisher-dawn-meyerriecks.html.

Tangredi, Sam and George Galdorisi. Eds. 2021. *AI at War: How Big Data, Artificial Intelligence and Machine Learning are Changing Naval Warfare*. Annapolis, MD: Naval Institute Press.

Tucker, Patrick. 2015. "Meet the Man Reinventing CIA for the Big Data Era." *Defense One*. Accessed April 12, 2022. https://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453.

Van Puyvelde, Damien, Stephen Coulthart, and Shahriar Hossain. 2017. "Beyond the Buzzword: Big Data and National Security Decision-making." *International Affairs* 93 (6): 1397–416.

Vella, Matt. 2016. "Tim Cook: 'We Will Not Shrink from Our Responsibility'." *Times*. Accessed March 2, 2022. https://time.com/4266246/tim-cook-apple-event/.

Vergun, David. 2021. "General Says Artificial Intelligence Will Play Important Role in Network Defense." Accessed July 20, 2022. https://www.defense.gov/News/News-Stories/Article/Article/2805760/general-says-artificial-intelligence-will-play-important-role-in-network-defense/

Villasenor, Joh. 2020. "Soft Law as a Complement to AI Regulation." *Brookings*. Accessed March 2, 2022. https://www.brookings.edu/research/soft-law-as-a-complement-to-ai-regulation.

Vinci, Anthony. 2020. "The Coming Revolution in Intelligence Affairs." *Foreign Affairs*. Accessed November 3, 2021. https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs.

Vogel, Kathleen, Gwendolynne Reid, Christopher Kampe, and Paul Jones. 2021. "The Impact of AI on Intelligence Analysis: Tackling Issues of Collaboration, Algorithmic Transparency, Accountability, and Management." *Intelligence and National Security* 36 (6): 827–48.

Washabaugh, Eric. 2021. "The Robot, the Targeter and the Future of US National Security." *Cipher Brief*. Accessed February 3, 2022. https://www.thecipherbrief.com/the-robot-the-targeter-and-the-future-of-u-s-national-security.

Weindling, Mark. 2022. "AI: Machine Learning vs. Expert Systems." *Neurocern*. Accessed January 3, 2023. https://www.neurocern.com/ai-machine-learning-vs-expert-systems.

White House. 2022. "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." Accessed January 4, 2023. https://www.whitehouse.gov/ostp/ai-bill-of-rights.

Williams, John. 2021. "Locating LAWS: Lethal Autonomous Weapons, Epistemic Space, and 'Meaningful Human' Control." *Journal of Global Security Studies* 6 (4) 1–18.

Younger, Alex. 2018. "'C' Speech on Fourth Generation Espionage." Accessed August 6, 2023. https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage.

Zegart, Amy. 2022. *Spies, Lies, and Algorithms: the History and Future of American Intelligence*. Princeton, NJ: Princeton University Press.

Zeng, Jinghan. 2020. "Artificial Intelligence and China's Authoritarian Governance." *International Affairs* 96 (6): 1441–59.