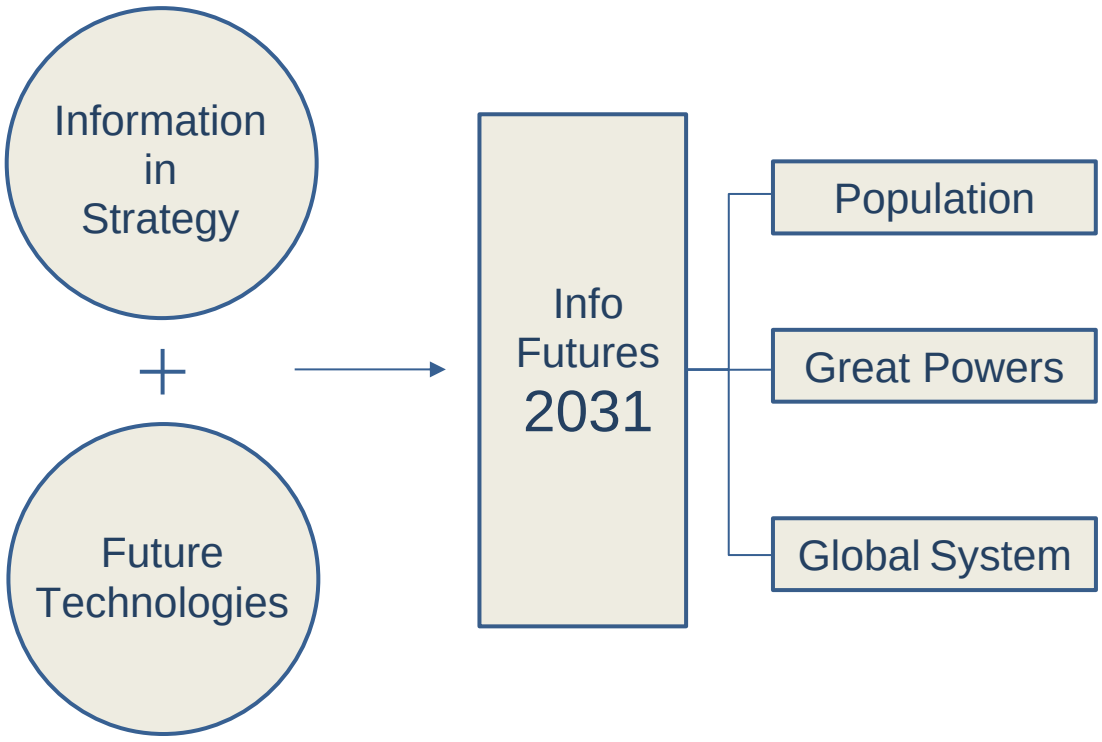
Intelligent Biology.

The future character of information in strategy:
forged by cognition and technology

Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group

Nicholas D. Wright

– v1 August 2021 –



The United States Department of Defense Joint Staff Strategic Multilayer Assessment Group sponsored this research as part of a project for Headquarters Air Force, to examine Integrating Information in Joint Operations (IIJO). For further information contact Intelligent Biology (www.intelligentbiology.co.uk).

This report is one of a coherent family of *Intelligent Biology* products that together provide a framework for successful influence across the spectrum of competition, including the gray zone. All are available www.intelligentbiology.co.uk, including:

- Wright, ND (2019, v3) ***From Control to Influence: Cognition in the Grey Zone***, Intelligent Biology.
- Ed. Wright ND, (2018) ***AI, China, Russia and the Global Order****: Technological, Political, Global, and Creative Perspectives,* U.S. Dept. of Defense Joint Staff.

About the author

Dr Nicholas Wright is affiliated with Georgetown University, University College London (UCL), Intelligent Biology and New America. He combines neuroscientific, behavioral and technological insights to understand decision-making in politics and international conflict, in ways practically useful for policy. He works with Governments. He has academic and general publications. He has a medical degree from UCL, a BSc in Health Policy from Imperial College London, Membership of the Royal College of Physicians (UK), and an MSc and PhD in Neuroscience from UCL.

Acknowledgements

The author thanks Todd Veazie, Wyatt Hoffman, Larry Kuznar, Steven Feldstein and others for helpful comments. All errors remain the author's.

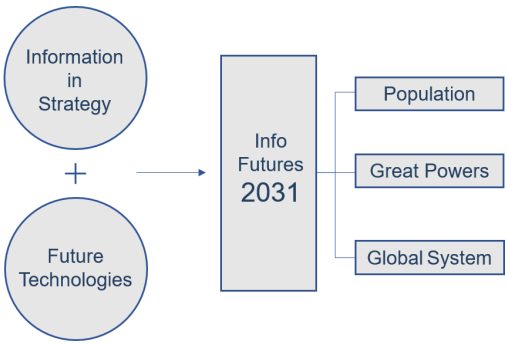
Contents

Executive summary

The basic cognitive *nature* of how human brains process information hasn't changed for millennia, including how we use information in strategy. Information is crucial for strategy aimed at others, whether that is outwitting adversaries or cooperating with allies. And even a superb strategy must be conveyed to one's own people. Humans remain central. But drivers like technology change the *character* of communication, societies and how we use information in strategy. This report examines key future technologies—including Artificial Intelligence (AI)—to ask:

What will be the future character of information in strategy in 2031?

To answer this question we follow a simple equation: Information in strategy (Part I) plus key technological drivers (Part II), are then combined to anticipate the character of information in strategy (Part III).



Part I. Information in strategy

Strategy is the art of creating power, for which information—defined as meaningful data—is central. But "information" is not a monolithic entity, and a piece of information's impact rests on its specific features.

Recommendation: Harness the **key features of information** (e.g. its degree of surprise), grounded in cognitive and other evidence, to cause intended effects.

Moreover, information alone is not enough. Consider the chain from *data* as a "raw material" processed into *information*; then *knowledge* (ordered sets of justified enough beliefs); and *wisdom* (broader context for more holistic judgements).

Recommendation: Digital **data** is exploding, which AI now turns into **information** – but the US can derive a key edge from enhanced **knowledge** and **wisdom**, operationalized via approaches like Jointness and Net Assessment.

Part II. Future technologies for 2031

Six key areas will drive change: software (e.g. AI); hardware (e.g. 6G); biology; outer space; who commands the tech (e.g. digital sovereignty over "big tech"); and who invents and builds the tech (e.g. more civilian than military). China is already a peer-innovator in AI.

Part III. Anticipating the character of information in strategy in 2031

Finally, we combine information in strategy and future technologies. We focus on three scales—populations, great powers and global systems—that are all crucial for US success with information in 2031.

Populations in 2031: facing domestic and foreign information threats.

- **Digital boundaries and managed openness:** Digital tech trends will have made the merger across the boundary between "domestic" and "foreign" information spheres *deeper* for most populations (e.g. in the US, UK or India). But countervailing political forces will also make digital boundaries around populations *lumpier*, in that the increased integration will be greater in some relationships (e.g. US-Australia) than in others (e.g. US-Russia) and in some sectors (e.g. healthcare) than others. How can the US defend and generate

advantages when operating across this deeper and lumpier boundary?

Recommendation III.1. Operationalizing plans like the Interim National Security Strategic Guidance (INSSG; Biden, 2021) to **merge domestic and foreign policy** must anticipate the **deeper and lumpier boundary** between them in 2031. A framework of **"managed openness"** generates advantages from this new terrain, e.g. when defending forward in cyber, or building secure networks with allies to enable the open connections that drive innovation.

- **Defending populations in 2031:** The US population faces threats from adversaries and other destabilizing forces that use information to sow discord, exert influence and obtain valuable knowledge. They will use new tech like AI.

Recommendation III.2. Responding effectively to information threats to the US population will require new human, technical and organizational capabilities. These are captured by a strategy built on "**3 Ds**": **Detect, Defend**, and **Democratic compatibility**. All three D's are necessary, and none is sufficient.

Great Powers in 2031: China-US escalation scenarios and war.

- **Signaling in escalation scenarios:** Signaling information between great powers during **crises** will change, which if unanticipated may cause inadvertent escalation. China will, for example, increasingly see US threats to its digital authoritarian systems (e.g. for "social credit") as threats against regime stability, which the US may poorly understand. More broadly, AI will bring vastly more true and false information, but little enhanced wisdom.

Recommendation III.3a. Anticipate the character of deterrence and escalation management in 2031, as the **character of "fog" and thresholds change**.

Recommendation III.3b. Enhance US capabilities for **knowledge** and **wisdom** – operationalized to harness vastly more **data** and **information**.

- **Plan for "Day 100" and remember "Day 2193" of a great power war:** Great power wars often last years or decades. Britain's World War Two lasted 2193 days. If a limited China-US conflict broke out then a years-long war is not unlikely, even in our nuclear age, with big effects for the US use of information.

Recommendation III.4a. Recognize that **long wars happen** between great powers and explicitly **plan for eventualities at Day 100 and beyond**.

Recommendation III.4b. By the time a war erupts it may be **too late** to create much of what is needed for a long war. Thus, anticipate key needs for a long war, and also build critical systems for resilience not just maximum efficiency.

Global information systems in 2031: global strategy for global competition.

- **Power from US centrality in global information flows:** US centrality in global information flows. Partly inherited from Britain, immense hard work maintained this strength. For 2031, 6G could threaten the Five Eyes' advantage in telecoms; while digital currencies like Monero, Diem, an "e-euro" or "e-renminbi" threaten US centrality in financial information flows. China now benefits from *its* centrality in global supply chain information flows.

Recommendation III.5. Reinforcing the status quo **and** adapting fast enough to tech change are both key. At global scale this requires **"managed openness"** to build innovative responses domestically and via networks—from the closest allies on outwards—that balance security and the benefits of connection.

Introduction

"Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?" – T S Eliot

[Winston Churchill had] "that all-embracing view which presents the beginning and the end, the whole and each part, as one instantaneous impression" – Eliot Cohen

"Knowledge is power." – Attributed to Francis Bacon

"The dive bombers will form a flying artillery, directed to work with ground forces through good radio communications … tanks and planes will be [at the commander's disposition]. The real secret is speed – speed of attack through speed of communication" – Erhard Milch, German air-force general, pre-war conference on Blitzkrieg tactics[1]

In 1940 German forces not only had the latest technology to match the Franco-British armies, but their *Panzer* divisions and *Blitzkrieg* harnessed that technology far more effectively. They harnessed information internally to better integrate and coordinate their forces. Meanwhile, *Blitzkrieg* used the speed of information bombarding an adversary to shock, disorient and defeat that adversary.

Having and harnessing the latest technologies to use information can be crucial across the spectrum of human competition, from peace through the gray zone to war. In the years of gray zone competition before 1939, Germany skillfully manipulated information—deception, surprise and propaganda internally and externally—to take them from the profound military weakness imposed by the 1919 Versailles Treaty, through to the military and strategic strength that smashed the allied armies in war.

Failure to anticipate the changed character of conflict was catastrophic for the allies – and a good part of that was failing to anticipate the changing character of how information would be used. The character of information use in 1939-45 differed from 1914-1918, and so too did the years of gray zone conflict before World War One differ from those preceding World War Two.

But Britain better harnessed information for its vital defensive shields in 1940. The world's first integrated air defense system, Fighter Command, used pioneering technology and superior coordination of air assets to win the Battle of Britain: Hitler's first major defeat. Sonar helped win the Battle of the Atlantic. Cracking the German Enigma codes gave a defensive and offensive edge. Prime Minister Churchill engaged intensely with President Roosevelt to bring the US into the fight against Hitler's war machine – and both leaders' ability to step back from the relentless frenzy of information that they faced, to see the big picture, shaped history.

Of course, the nature of information use was not new in either World War Two or its preceding gray zone competition. *Panzer* forces combined arms and created

[1] Quoted in (Keegan, 1993, p. 370).

surprise, but so did Napoleon, Hannibal or Alexander. Carl von Clausewitz described the “fog of war” in Napoleonic conflicts, but it applied just as well to every major contest before or after, and will surely pervade future contests conducted via a panoply of AI-enabled systems. Failure to anticipate the changing character of information in strategy can be disastrous, but to anticipate what may change also requires grasping the unchanging nature of information in strategy – for which human cognition provides a solid bedrock (Box 1). Technology changes, but the humans on the receiving end—and on the giving end—of strategy remain human.

US success requires both understanding the *nature* of information in strategy, for which cognition is a solid bedrock, and anticipating its *character* in our coming epoch, which is aided by a grasp of technology. Of course, neither cognition nor technology explain everything, but they explain much of what matters. This report looks ahead 10 years to 2031, which is near enough for sensible predictions yet far enough for significant differences to emerge.

The report follows a simple equation: information in strategy (Part I) plus key technological drivers (Part II), which are then combined to anticipate the character of information in strategy (Part III).

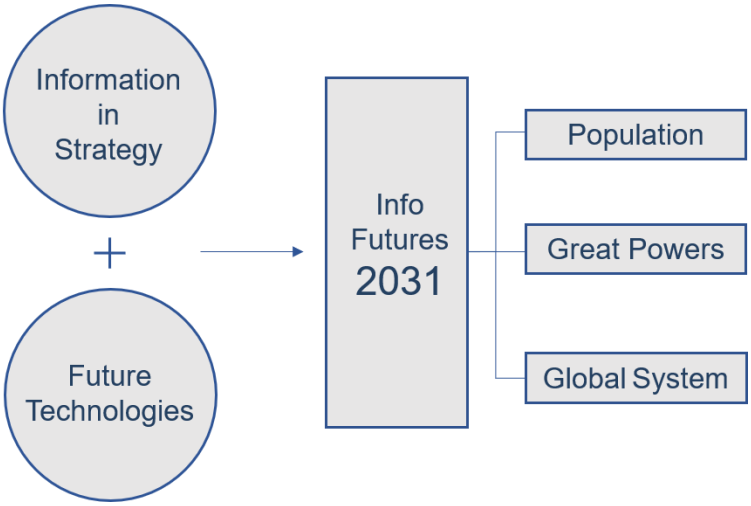


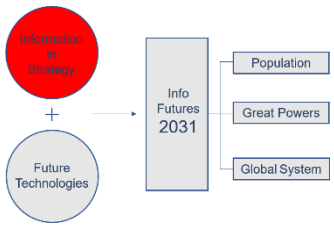
Figure 1 Overview of this report.

Box 1 Changing character and unchanging nature of conflict between humans

A distinction is commonly drawn between the character and nature of war. Scholar Colin Gray, for instance, wrote that “*Many people confuse the nature of war with its character. The former is universal and eternal and does not alter, whereas the latter is always in flux”*.

A key reason for the consistent nature of human conflict is that it remains a strategic interaction between humans, between human psychologies. As Gray further notes: *“The stage sets, the dress, the civilian and military equipment, and some of the language are always changing, but the human, political, and strategic plots, alas, remain all too familiar.” … “Interstate war and warfare continue to plague the human race. Even war between great powers is possible, given the political fuel lurking in the twenty-first century in the deadly and familiar classical Thucydidesan categories of ‘fear, honor, and interest.’”* (Gray, 2010, pp. 6, 11, 12)

Part I. Information in strategy: its nature and character



Information can be defined as meaningful data.[2] Used more colloquially, information often refers to any medium that presents knowledge or facts. No perfect, universal definition of information can ever exist.[3] Information takes many forms, such as genetic information stored in our DNA, neural information encoded in the firing patterns of brain cells, written information on ancient cuneiform tablets, birdsong, or digitally encoded information on a hard-disk or the internet.

How does information matter for strategy? Strategy, as Lawrence Freedman describes in his book *Strategy* (2013), is the art of creating power. Turning to definitions of power, that can be exerted in two ways: one is to *influence* another's choice to get a desired outcome (deterrence is one example of such influence); and a second is to exert *control* by removing another's capability to choose (e.g. by brute force).[4]

Thus, here in Part I:

- We first consider information in strategies to *influence* others, and then in strategies to *control* others. For each, we consider its nature and character, as we do throughout Part I.
- We next consider how information is used in *one's own side*, as even the most brilliant strategy must be communicated to those who must carry it out.
- But although information matters, information is very far from the only thing that matters – and only by understanding what information is *not* can we see how to combine information effectively with other factors for strategy.
- The final subsection outlines some key conditions that shape the way technology affects the character of information in strategy.

Information in strategy to influence others

To influence an Afghan farmer not to grow poppy, the influencer must look from *the audience's* perspective to consider how the audience receives information related

[2] This simple definition is compatible with recent US doctrine. The Joint Concept for Operating in the Information Environment (Department of Defense, 2018), defines ***Information*** as: "A particular arrangement or sequence of things conveys specific information. Information is stimuli that have meaning in some context for its receiver." It also defines the ***Information Environment (IE)***. "The IE is comprised of and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The IE also includes technical systems and their use of data. The IE directly affects and transcends all OE [Operating Environment]."

[3] Consider three reasons: (1) Even within mathematically specifiable approaches it is difficult to define. As the "father of information theory", Claude Shannon wrote "It is hardly to be expected that a single concept of information would satisfactorily account for the numerous possible applications of this general field." Quoted in (Floridi, 2010). (2) Within the security field, different countries—e.g. the US, Russia and China—can have very different concepts of information (Giles & Hagestad, 2013). (3) Diverse fields from mathematics to physics, biology and psychology each bring their own distinctive interpretations.

[4] Thomas Schelling, for example, distinguished between "coercion" and "brute force" (Schelling, 1966).

to that course of action and its alternatives.[5] If the aim is to deter a hostile state, i.e. influence it not to act, then the influencer must estimate how the hostile state perceives information about the costs and benefits of acting – and of not acting.

I define influence as a means to affect an audience's behavior, perceptions or attitudes. Influence can be achieved by, for example, deterrence, persuasion, or the use of hard or soft power. Influence does not only include "soft" means, but also the use or threat of hard power. The *nature* of influence remains unchanging in large part because it rests on cognitive foundations.

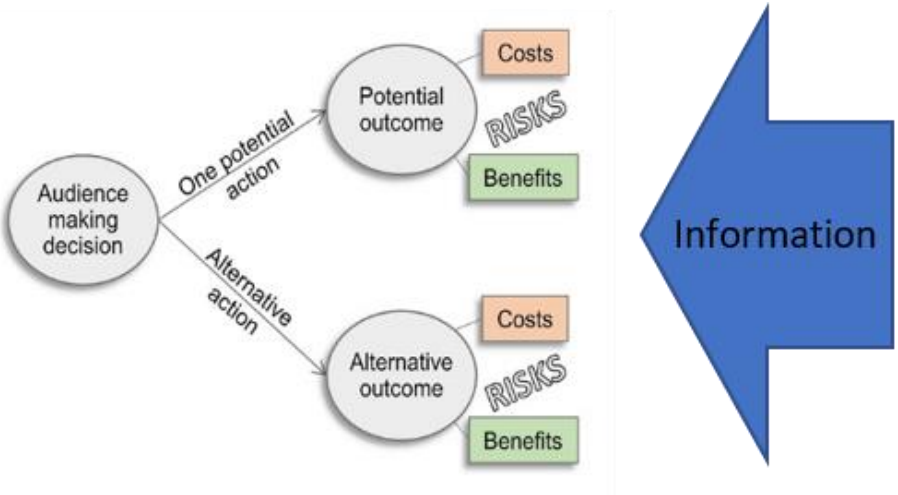


Figure 2: The Audience Decision Process. The audience's decision calculus must be at the heart of planning to use information in strategies to influence others. Practical tools, based in evidence, can help put oneself in the audience's shoes (e.g. the "checklist for empathy" in Wright, 2019, v3, From Control to Influence, www.intelligentbiology.co.uk).

Deterrence is one form of influence and illustrates these cognitive foundations, as do other forms of influence like "compellence" or escalation management.[6] In the US case, for instance, the DoD Dictionary of Military and Associated Terms[7] defined that *"Deterrence is a **state of mind** brought about by the existence of a credible threat of unacceptable counteraction"* [emphasis mine] from the 1990s until the past few years and now defines deterrence as *"The prevention of action by the existence of a credible threat of unacceptable counteraction and/or **belief** that the cost of action outweighs the **perceived** benefits"* [emphasis mine]. This reflects many leading Western scholars, such as the American Patrick M. Morgan, who writes that *"Deterrence is undoubtedly a psychological phenomenon, for it involves convincing an opponent not to attack by threatening harm through retaliation…"* (P. M. Morgan, 1985, p. 125), or French thinker Bruno Tertrais who writes that *"deterrence is fundamentally a psychological process."* (Tertrais, 2011)

[5] Please see the previous SMA report Wright (2019), v3, *From Control to Influence: Cognition in the Grey Zone*, for discussions of the rationale and how to implement influence. Download at www.intelligentbiology.co.uk.
[6] For a discussion see Wright (2019) *From Control to Influence.*
[7] Department of Defense Dictionary of Military and Associated Terms, Joint Publication, as of January 2021. Earlier definition present in 1994 edition and up to 2011, but not by 2016.

Neither is this cognitive foundation purely Western, as Chinese doctrine also has psychology at the core of its thinking on deterrence. Consider an authoritative publication like *The Science of Military Strategy* (Peng & Yao, 2005, p. 214). The authors state that *"[D]eterrence requires turning the strength and the determination of using strength into the information transmitting to the opponent, and to impact directly on his* ***mentality*** *in creating a* ***psychological pressure*** *to shock and awe the opponent." [emphasis mine]. "There are three basic elements to carry out deterrence: First, appropriate military strength available; second, resolve and will to use force; and third persuading the opponent to perceive such strength and resolve."* (Peng & Yao, 2005, p. 18)

But all pieces of information aren't equal, and their strategic impact depends on specific features. Many such features of information arise from basic human cognition and so form a solid bedrock to anticipate the *nature* of information in strategy – although it is also crucial to appreciate that their *character* changes with technology.

Surprise, for example, is a basic feature of information in strategy that continues to matter as much in social media as it did for Sun Tzu – *and* to harness this feature of information effectively requires anticipating how its character will change. It remains central because it is a fundamental feature of how the brains of humans and other animals learn and understand the world—where it is often discussed as "prediction error"—and it is probably the most significant neuroscientific finding of the past quarter century (see e.g. (Wright, 2019c)). Manipulating surprise and unexpectedness to cause intended information effects was central to military thinkers from seminal interwar airpower theorists like Giulio Douhet to Cold War scholars like Thomas Schelling (Wright, 2014) and has been harnessed by practitioners from *Panzer* commanders to North Korean leaders (Wright, 2018, pp. 17–20).

The flip side of surprise is predictability. Recent neuroscience work suggests predictability overall is desirable in itself (Friston, 2010). This concurs with David Kilcullen's argument that generating predictability is central to successful counterinsurgency (Kilcullen, 2013). The foundation of his book "*Out of the Mountains*" is the "theory of competitive control," where "populations respond to a predictable, ordered, normative system, which tells them exactly what they need to do, and not do, in order to be safe."

Surprise is key for social media messaging. ISIL skillfully kept their offering fresh and attention grabbing, for instance by using novel, horrific types of execution and execution coverage (e.g. see Wright, 2015). A large recent MIT study on the spread of fake news looked at some 126,000 stories tweeted by about 3 million people more than 4.5 million times, and showed that media's novelty and surprise are key for driving its spread (Vosoughi et al., 2018). Taylor Swift became the youngest of America's richest self-made women in large part through her skillful use of social media, in which a central feature was harnessing surprise (Singer & Brooking, 2018, Chapter 6). As Taylor Swift described:

> *"I think forming a bond with fans in the future will come in the form of constantly providing them with the element of surprise. No, I did not say shock I said surprise. I believe couples can stay in love for decades if they just continue to surprise each other, so why can't this love affair exist between an artist and her fans."*

Thus, analysts or strategists trying to anticipate the future character of information must think through how new technologies will affect surprise and unexpectedness. For the audience ask: "*What are their key expectations, and what may violate them?* The more unexpected a perceived event is, the bigger its psychological impact. When crafting messages, creativity is crucial: *"How can we manage novelty and unexpectedness?"* A messenger's salience can also be enhanced when they are more unexpected. Box 2 describes further key features of information for strategy.

Recommendation I.1. Harness the *key features of information for strategy* (see Box 2, e.g. its degree of surprise) to cause intended, and avoid unintended, effects.

Recommendation I.2. To anticipate the *future character* of information in strategy, consider each of these features of information in strategy and *ask how technology may change its character.*

Box 2 Core features of information in strategy

Core features of information that matter for strategy can be identified from extensive cognitive science and real-world research – as described in the previous SMA report, *From Control to Influence*, with discussions and detailed appendices containing the evidence base for population and states (Wright, 2019a). Available at www.intelligentbiology.co.uk.

These core features of information may be grouped in various ways, but for simplicity and ease of operationalization here we group them according to "Audience", "Message" and "Messenger." Key features of the information remain key as they are part of the nature of strategy between humans, although the character of how will they manifest differs.

Audience

A set of practical questions can help to estimate the audience's perceived costs and benefits for their potential alternative actions in a given context. These may include:

Self-interest: *"What material benefits may they gain or lose?"* The importance of self-interest was shown by the switching allegiances of Sunni groups during the 2007 Surge in Iraq, which involved U.S. rewards and threats of punishment.

Fairness: *"How fair will it be seen from the audiences' perspectives?"* Humans typically pay costs to reject unfairness and pursue grievances.

Fear: "Do they fear for their security and why?"

Identity: *"What are their key identities?"* Humans are driven to form groups ("us", the "in-group") that are contrasted against other groups ("them", the "out-group"). Individuals also often hold multiple overlapping identities.

Status: *"How may this affect the audience's self-perceived status?"* E.g. For key audiences in Afghanistan, joining the Taliban had high status.

Expectations: "*What are their key expectations, and what may violate them?* The more unexpected a perceived event is, the bigger its psychological impact.

Context, opportunity and capability. "*What opportunities and capabilities does the audience perceive it has for its potential alternative actions?"*

Message

After developing an in depth understanding of the target audience, successful messages must be developed.

*(1) When **fashioning messages**, consider the following: information must be simple, credible and creative* (e.g. manage novelty and unexpectedness).

*(2) **Content of messages:** Messages should address key audience motivations such as identity, fairness, fear or self-interest (e.g. see checklist for empathy above).*

*(3) It is vital to consider the **communication context**, not the message content alone.* Humans are attuned to evaluate information by comparing stimuli with other stimuli or options, so use **contrast effects** to make the desired option the better option. **Timing** matters, as does **standing out against noise.**

Messengers

Finding and developing the right messengers of information is vital.

Firstly, policy must consider three key messenger characteristics: trust, salience and capability. One way is to manage the **unexpectedness of messengers**. Iranian President Rouhani's unexpected use of 2013 Twitter diplomacy changed the political climate and enabled successful nuclear talks (Wright & Sadjadpour, 2014). Repeated exposure to the same messenger can lead audiences to habituate.

*Second, understanding **networks** can help identify effective messengers.* Face-to-face, family, social media and other networks can provide key access to audiences.

Information in strategy to control others

The second way to exert power is *control*, which removes another's capability to choose. Information may again be central, as shown by the three following cases.

One case is using information to prevent an adversary receiving crucial information. World War Two British bombers, for instance, dropped metal strips called "chaff" as a countermeasure to blind German radar. Now, computer network operations and electronic warfare (EW) can be used for jamming across the battlefield (Porche et al., 2013) including space (Harrison et al., 2021).

What will be the future character of such operations? In the future we can anticipate increased convergence of cyber and EW as we move to a globe of wirelessly connected 5G "networks of smart things", which will be compounded as we move towards 6G by 2031 (see Part III, Box 6). We can also anticipate that blinding or degrading adversary AI-enabled sensors will be key. AI must currently learn from datasets and an adversary's AI may be blinded to cleverly prepared "edge cases."[8]

[8] AI multiplies vulnerabilities in systems. Systems can be trained on a corpus of expected environments, but if the other side generates "edge cases" that the defender failed to imagine, the receiver's AI may exhibit behavior favorable to the hacker. One can describe an edge case as a problem or situation that occurs only at an extreme (maximum or minimum) operating parameter. For elaboration see (Libicki, 2019).

Preparation of the competitive space will increasingly involve manipulating or exploiting weaknesses in the data on which an adversary's AI trains (Hoffman, 2021).

Another case is to disrupt the adversary's internal flows of information required for their decision-making and coordination. Again this may involve traditional computer network operations or, in future, feeding poisoned data to their AI. Another key method is to sow discord and disruption amongst the humans in an adversary's force and its support networks, in order to degrade their collective capabilities – as we see with Russia and other destabilizing forces.[9]

A third case is "shaping" adversaries via information, which may take place over years and aims to materially change an adversary's relative capabilities (not just to influence what they choose to do with their capabilities). Stuxnet is one example, where the US is suggested to have aimed to delay the Iranian nuclear program by damaging it, in addition to also making Iranian scientists doubt their own abilities (Buchanan, 2020). China steals US commercial secrets to build its own innovation base and so tilt the economic balance of power in its favor (Kazmierczak et al., 2019). US industries can be undermined. China, in common with Western countries, also steals military secrets to enhance its own relative capabilities (Sanger, 2018).

Recommendation I.3. Avoid the "drunkard's walk" lurching from notions during the US unipolar moment that only control matters (because the US can dominate any sphere of contest) to ideas that only influence matters – both are crucial for success and both require distinct uses of information.

Information within one's own side is vital for strategy

Successful strategy is as much about one's own side as the other's side. Consider the following three ways in which information is crucial.

Firstly, to communicate strategies to the humans in the force. As Lawrence Freedman writes "[S]hrewd judgment is of little value unless it is coupled with an ability to express its meaning to those who must follow its imperatives." (Freedman, 2013, p. 614) We need not subscribe to a "great man" theory of history to recognize that leadership, vision and good human communicators will always be a factor – which can be (partly at least) selected for and taught (Jackson et al., 2020; Spain, 2020; Straus et al., 2018).

Second, human cognition is a tool for executing strategy. Consider the past century of Russian information operations, which up to the modern-day Internet Research Agency has harnessed cognition as a tool to implement its information operations. The scholar Thomas Rid describes how Cold War Soviet "Active Measures" required not only vast, well-funded and highly organized bureaucracies, but also talented, motivated and creative humans to produce the materials and broader campaigns (Rid, 2020). That requirement remains now for those seeking to use the sophisticated AI-enabled "deepfakes"—as described in the companion report for this SMA effort (Wright 2021, *Cognitive defense*, www.intelligentbiology.co.uk)—

[9] See the companion report for this SMA effort: Wright (2021) *Cognitive defense of the Joint Force in a digitizing world.* Available at www.intelligentbiology.co.uk

and will continue in the future as it is part of the unchanging *nature* of using information in strategy.

But the *character* of how to get the most out of one's own humans, so that they communicate and process information effectively within the organization – that changes with new technological and other innovations. In the near future, for example, rolling out AI means effectively sharing information within human-machine teams, which relies as much on understanding human cognition and organizational factors as it does on the technological parts of the team.

Indeed, harnessing these factors together—people, technology and organizations—under the character of the age can provide a huge edge. Consider a pivotal historical case, described by the leading military historian Michael Howard:

> The Prussian, and later German, *"General Staff was perhaps the great military innovation of the nineteenth century. …With the increase in the size of these armies brought about by the development of railways the problems of both peacetime preparation and wartime command and control were greatly increased. In the French, Austrian, and British armies staff officers … became little more than military bureaucrats … . [Prussia's Helmuth von] Moltke [who was Chief from 1857-1888], on the contrary, turned them into an élite, drawn from the most promising regimental officers, trained under his eye... . [Crushing the French armies in] 1870 was as much a victory for Prussian bureaucratic methods as it was for Prussian arms … . The romantic heroism of the Napoleonic era … was steam-rollered into oblivion by a system which made war a matter of scientific calculation, administrative planning, and professional expertise."* (Howard, 1976, pp. 100–101)

Every state in continental Europe copied this model after Prussia's stunning successes from 1864-70, as did Britain and the US a little later. Better central use of information and better decentralized use of information were key.

Organizational adaptation must go hand-in-hand with advancing technologies for information production, communication and processing. This helps organizations be more robust to the character of the "fog of war" using current technologies. It also helps with that other Clauswitzean challenge of "friction" – the Prussian General Staff, for instance, smoothed out railroad logistics to create devastating power. AI now offers huge potential for tasks like logistics, but will US organizations harness it?

Thus, information is crucial for one's own side in a third way: organizations reap strategic advantage if they can adapt their information processing to effectively harness the nature of humans and the character of technology. No single intervention alone is sufficient to effectively manage change in organizations. Innumerable schemas seek to capture the multiple factors that matter for managing change, of which a good illustration is the well-known and decades-old "McKinsey 7S model" that looks at: staff, structure, strategy, systems, skills, style, and shared values.

Recommendation I.4. Apply realistic views of human cognition, organizations and technology to the internal dimensions of strategy – which in our coming epoch requires effective leadership, human teams, human-machine teams, and human-organizational relationships.

- For practical tools to provide realistic views of human cognition, grounded in evidence, see e.g. Chapter 2 in Wright (2019) *From Control to Influence*, and for review in combination with culture and organizational factors see Chapter 4 in Wright (2019) *Global strategy amidst the globe's cultures*. Both downloadable at www.intelligentbiology.co.uk.

What information is not: decision-making and action

But although information matters, it is far from the only thing that matters, and only by understanding what information is *not* can we see how to combine information with other factors for effective strategy. So, what is ***not*** information?[10]

Firstly, information is neither decision-making nor action. Consider an organism, anywhere from an *Amoeba* to a nematode worm to a human. "Information" in a stimulus can "influence" how an organism "decides" between options, and if those options are "actions" then the choice may be observed as "behavior." Within an organism "information" can undergo "computations" that are involved in decision-making. But while all these concepts in inverted commas are related, they are all distinct. This does not belittle the importance of information, but places it in context.

So what? A key implication is that we should not get too carried away by the importance of information. The central aim of influence, for example, is to affect others' decision-making. To achieve that goal, a key idea from many disciplines is to put yourself in the other's shoes – an idea based in considerable evidence.[11] Placing the other's decision-making at the heart of the influence effort—not "information"—will most likely remain the most fruitful guiding principle.

What information is not: data, information, knowledge, wisdom

Furthermore, information is only one stage within a chain including data, information, knowledge and wisdom – and is not itself the other links in the chain.

Despite libraries of scholarship examining each term, no perfect definition can exist of any of them, nor of their relations. But a bird's eye view gives two benefits:

- it shows why we care so much about "big data" and AI now; and
- it highlights areas where the US can gain significant strategic advantage.

Figure 3 below is my effort to relate these concepts and how they are currently changing through technology[12], but the poet TS Eliot is more elegant:

> *"Where is the wisdom we have lost in knowledge.*
> *Where is the knowledge we have lost in information?"*

---

[10] Borderline cases of what falls inside or outside "information" will always exist, not least because as described above no perfect definition of information can exist – but such distinctions are still meaningful and useful. An analogy is baldness. My father is now a bald man and when younger had a full head of hair. It is difficult to say when *precisely* he went from the one to the other, but that does not mean the category 'bald' is not a useful category.

[11] Reviewed in Wright (2019) v3, *From Control to Influence*. Download at www.intelligentbiology.co.uk

[12] In the management literature a well-known data-information-knowledge-wisdom hierarchy has been proposed (Ackoff, 1989), although I agree with (Weinberger, 2010) that the four concepts are much broader than those used in the management literature and that a hierarchy is not the best format. Hence, for example, I use backward arrows to show how top-down as well as bottom-up links matter. This is also more consistent with modern neuroscience accounts, e.g. (Friston, 2010). For discussions of the management literature, see e.g. (Rowley, 2007).

Carl von Clausewitz also described this chain, writing in his chapter about "Intelligence in War"

> *"By 'intelligence' we mean every sort of information about the enemy and his country …. Many intelligence reports in war are contradictory; even more are false, and most are uncertain. What one can reasonably ask of an officer is that he should possess a standard of judgement, which he can gain only from knowledge of men and affairs and from common sense."* (Clausewitz, 2008, p. 64) And as he discusses earlier:
>
> *"To bring a war, or one of its campaigns, to a successful close requires a thorough grasp of national policy. On that level strategy and policy coalesce: the commander-in-chief is simultaneously a statesman. [King] Charles XII of Sweden is not thought of as a great genius, for he could never subordinate his military gifts to superior insights and wisdom, and could never achieve a great goal with them. … We argue that a commander-in-chief must also be a statesman, but he must not cease to be a general."* (Clausewitz, 2008, p. 59)

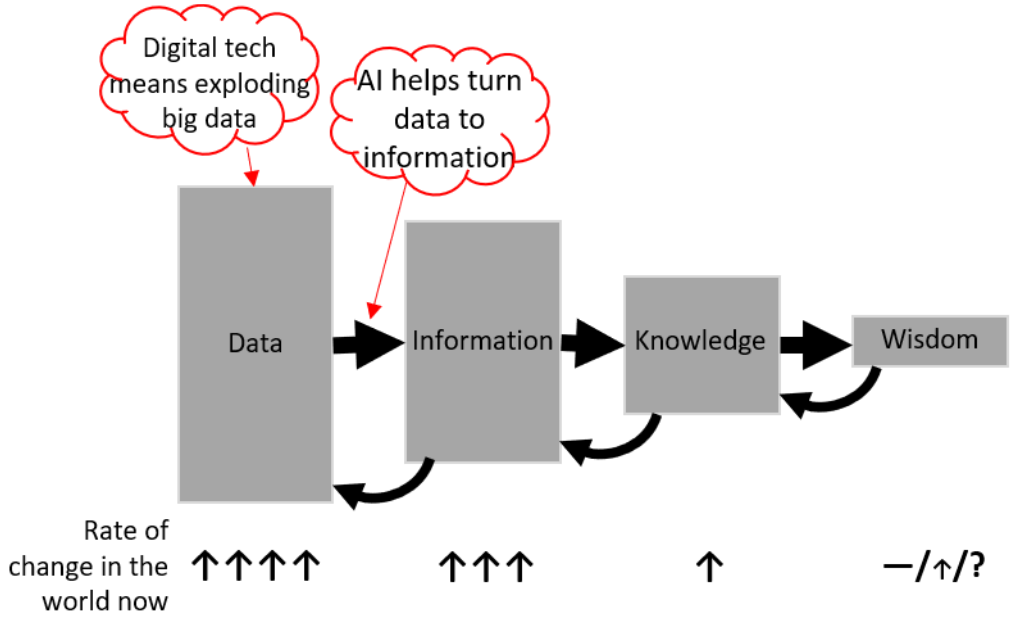


Figure 3 Data, information knowledge and wisdom. The character of technology now means that data is expanding very rapidly, which AI can now increasingly turn into information, but this only more slowly increases knowledge or wisdom.

Next we can go through each of the four links in the chain, which I illustrate with the example of a human gene.

Data are facts and statistics collected together for reference or analysis, in which a single "datum" is a distinction that makes a difference (e.g. a thing is red or blue, or a thing is present or absent) (Floridi, 2010, p. 23). They are quantities, characters, or symbols on which operations (or "computations") are performed by a "computer" such as a human nervous system or digital computer. Data require processing to be meaningful.

- E.g. The human genetic code is a 3 billion long string made up of four letters (C,T,G or A). It looks like this "…ATGCAAAAGTTCAAGGTCGTC…"

Information is meaningful data. It involves descriptions and is, usually, useful.

- E.g. Genes can be read from sections of the genetic code, such as those coding for eye color, cancers or early onset dementia.

Knowledge can be considered a more-or-less systematically ordered set of beliefs that are true and that we are justified in believing.[13] Knowledge is also often useful and, furthermore, humans often require experience to master a body of knowledge. Thus, a broader description is that "Knowledge is the combination of data and information, to which is added expert opinion, skills, and experience, to result in a valuable asset which can be used to aid decision making".[14]

- E.g. A physician considering a patient's genetic test result may combine that with the scientific literature plus information from the results of the patient's other medical tests, and so have knowledge of what a particular gene reveals about the patient's risk of cancer or dementia.

Wisdom involves broader knowledge that provides both context and also a humility about what is unknown, which enables a more holistic assessment of the multiple key trade-offs required in complex judgements (Box 3).[15]

- E.g. Now looking at that genetic knowledge in the broader context of a patient's family circumstances, past mental health, young children, religious beliefs and so on – what are the best (or least bad) ways of moving forwards?

To provide a military example across this chain, consider the following:

- *Data:* Pixels from Earth Observation satellites.
- *Information:* Vehicles counted, identified according to type and unit, and locations ascertained.
- *Knowledge:* Vehicles of this type, taken together with other new capabilities, recent history and changes in online discussions suggest a marked change in a competitor's military posture. They may be about to strike another actor.
- *Wisdom:* What does this new knowledge mean within that actor's broader socio-political context, or the broader regional and global contexts? As once commented[16] about the early days of the ISIL fight – the US can do all of this, but step back and look at the bigger picture and if that means we lose Turkey as an ally, then we have lost far more than we gained. A stunning tactical or even operational advantage may be a strategic detriment.

Finally, we can return to ask: So what?

---

[13] Knowledge and information are members of the same conceptual family, but knowledge enjoys a web of mutual relations that allow one part of it to account for another – so that once some information is available, knowledge can be built in terms of explanations or accounts that make sense of the available information (Floridi, 2010, p. 51). Knowledge as "justified true belief" has been a powerful definition since Plato, although the problems raised in Edmund Gettier's 1963 paper as to whether this is sufficient for knowledge have compromised that definition for many contemporary philosophers of knowledge (Ichikawa & Steup, 2018).

[14] European Framework for Knowledge Management, quoted in (Rowley, 2007).

[15] Wisdom is discussed across many diverse disciplines. For accessible discussions of wisdom in philosophy see e.g. (Ryan, 2020), in psychology see e.g. (Grossmann, 2017), in management e.g. (Rowley, 2007), and in functional genomics (Ponting, 2017).

[16] Comment by a very senior US decision-maker, relayed to this author and paraphrased here.

One benefit is to identify how technology affects the distinct links in the chain of data, information, knowledge and wisdom. Technology is vastly increasing the amount of data captured by our increasingly digital surroundings. Such "big data" is characterized by three "V"s, in that big data is high-volume, high-velocity and high-variety data (ICO, 2017). AI and other types of "big data analytics" are ever more able to process vast volumes of data into information. But AI is currently poor at dealing with context—which will continue without a new technical leap (Part III, Box 7)[17]—so that AI alone is poor at knowledge, let alone wisdom, despite their crucial importance for strategy.

Another benefit arises because all the distinct links in the chain—data, information, knowledge and wisdom—matter for US success, and this clarifies that the US should seek effectiveness or superiority at *every* link in the chain:

- The US must continue to lead in data and information, which are the most technology-heavy parts;
- The US must drive human-machine innovation and organizational innovation, in order to better harness AI-enabled information for integration into knowledge and wisdom;
- The US must further operationalize knowledge and wisdom, which is only partly about harnessing technology.

Recommendation I.5. Digital *data* is exploding, which AI now turns into *information* – but a key US edge can be to enhance *knowledge* and *wisdom*, operationalized via approaches like Jointness and Net Assessment.

How do you "operationalize knowledge" or "operationalize wisdom", and indeed doesn't the latter sound like an almost impossible aim?

Operationalizing knowledge: Knowledge can be enhanced at many levels in the Joint Force.

- Humans with knowledge of expert domains will always be needed. Consider humans with knowledge of cyber, which is a crucial need for both US national security organizations and the private sector. The US military can help fulfill that need by funded training programs at university level followed by practical experience – and indeed many private sector cyber jobs require practical experience that is difficult to acquire from purely academic training (Clarke & Knake, 2019). Knowledge often requires combining practical experience to academic study, so a practitioner can harness a web of facts, connections and understanding. Languages, area studies and deep cultural experience can also be crucial areas of comparative advantage for the US, with its unrivalled global networks.
- Institutional knowledge can also be enhanced, for example about US influence and information efforts. Government should develop a clearinghouse of validated (and rejected) influence measures. This could give

[17] Box 7 discusses AI's current strengths and weaknesses. A major advance in AI occurred around 2012, the first for decades, and we would need change of a similar magnitude to crack the challenge of context.

practitioners easy access to a database of measures tried and tested, including both successes and failures.[18]

- Potential future US advantages in knowledge may also arise from the US' uniquely vast troves of data from sources like submarines, aircraft carriers or global military logistics. Such data are the raw materials for information and then to deep knowledge – knowledge to which no other nation, with the partial exception of China, could aspire. Such knowledge will bring considerable power, if the US can harness it and keep it secure.

But knowledge alone, even though it is necessary, is also insufficient. Winston Churchill drew extensively on expert scientific advice, for instance, but was famously said to have observed that "scientists should be on tap, but not on top". So too with military knowledge, even when it is brilliant.

The German General Staff operationalized knowledge brilliantly in the nineteenth and early twentieth centuries, but they also deliberately limited how that knowledge was placed within a broader context. Chief of that General Staff, Helmuth von Moltke, has a good claim to be one of the nineteenth century's greatest and most successful military strategists. But if he had one serious weakness it was his almost total exclusion of political considerations. He accepted that war aims were determined by policy, but believed that once fighting began the military must be given a free hand: "strategy" must be "fully independent of policy." Facing a crisis over how to finally force French submission after the French armies—but not nation—had been defeated in 1870, Prussia needed a solution before she exhausted herself and so became vulnerable. But von Moltke seemingly would not see the bigger picture. As he reportedly said to crown prince Frederick William at the height of the crisis: "I have only to concern myself with military matters." (Freedman, 2013, pp. 106–107). Brilliance in the field alone is not sufficient – it was the politician Otto von Bismarck who drove judgements based on the bigger picture and led Prussia through that danger zone.

Operationalizing wisdom: See Box 3.

[18] Recommended in Wright (2019) *From Control to Influence* (Ch. 11) and earlier versions of that SMA report, as well as in the excellent Rand study on measuring influence efforts by (Paul et al., 2015).

Box 3. Operationalizing wiser judgements

Wisdom involves broader knowledge that provides both context and also a humility about what is unknown, which enables a more holistic assessment of the multiple key trade-offs required in complex judgements. Strategy and tactics are better when they see the big picture and the crucial details; the forest and the trees.

Operationalizing wisdom may sound fanciful, but it is a foundation of the US system of government. Consider the need to **reflect, to take a step back and think**. George Washington saw the need to operationalize this facet of wiser decision-making. Thomas Jefferson asked Washington why they should create a Senate. "Why did you pour that tea into your saucer?" replied Washington. "To cool it," said Jefferson. "Even so," responded Washington, "we pour legislation into the senatorial saucer to cool it." A reflective second chamber, a formal opposition, a free press – such remarkable devices help a country think about its own thinking. Imperfect, to be sure, but more durable than almost all other regimes over the past two centuries.

Integrating perspectives and knowledge from different parts of government has also been operationalized – it is the purpose of the US National Security Council. As in its founding 1947 Act: "The function of the Council shall be to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security". Again imperfect, but what went before could not provide the broader picture needed by a global power (McInnis & Rollins, 2021).

Net Assessment applies systematic methods to see more context and so enable wiser choices; to see "red" not in isolation but in the context of "blue" and perhaps "green" too. As much craft as science, it considers longer time-frames, wider strategic scope, socio-political context, and both behavior and organization. It uses qualitative and quantitative methods and appreciates complexity (Kuznar, 2021).

Operationalizing wiser decision-making at **many organizational levels**—locally and in combatant commands, not just in Washington—is also key. "The shooting side of the business is only 25 percent of the trouble," observed Sir Gerald Templar who successfully contained **counter-insurgency** in Malaya, "and the other 75 percent lies in getting the people of this country behind us." (Freedman, 2013, p. 188) Effective **civil-military integration** helps make for wiser counter-insurgency strategy and implementation. Effective responses to Russian, Chinese, Iranian or ISIL **gray zone campaigns now** requires integration within commands across "DIME", "PMESII" and so on (Robinson et al., 2018). Autocrats' multidimensional engagement is overloading democracies' ability to manage the challenge (Walker & Ludwig, 2021). Integration must not mean endless committees, but is often necessary.

Red-teaming can help organizations see their own practices and assumptions afresh, to help break complacency, inertia and groupthink (Zenko, 2015).

The many practical processes, institutions and practices that facilitate wiser decisions cannot be replaced by just more data, information or expert knowledge.

To be sure, even the wisest judgment can be horribly wrong: no individual or bureaucracy can integrate and anticipate everything (Freedman, 2013, p. 236); chance and rapid adaptation to changing contexts will always be key. But judgments can, as George Washington knew, be made wiser. And we must also seek to avoid what Winston Churchill (Churchill, 1948, p. ix) identified as a central failing of Western powers before World War Two: "unwisdom".

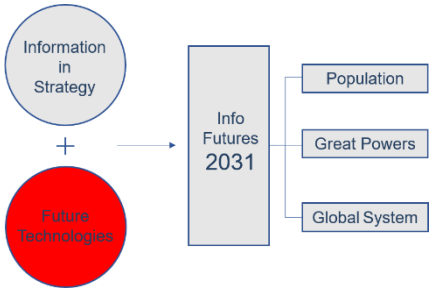
Conditions affecting how technology drives the character of information in strategy

This final subsection outlines some key *conditions* that shape the way technology affects the character of information in strategy. By analogy, if someone has a genetic predisposition to male pattern baldness, how likely they are to go bald depends on the *conditional* variable of whether they are male or female.

- **Domestic political regime type:** Different types of regimes may use the same technologies in different ways. A domestic political regime is a system of social organization that includes not only government and the institutions of the state but also the structures and processes by which these interact with broader society. The new AI-related technologies affect both authoritarian (e.g. China) and liberal democratic regimes (e.g. the US). However, the character of these technologies particularly favors the augmentation of surveillance, filtering, and prediction, and thus they more greatly enhance digital authoritarian systems of social organization (Wright, 2019b).
- Points along the **spectrum of competition** from peace through the gray zone to limited and total war. For example, gray zone conflict is necessarily *limited* conflict, sitting between "normal" competition between states and what is traditionally thought of as war. Thus, the central aim is to *influence* the decision-making of adversaries and other key audiences, rather than removing their capacity to choose using brute force in itself. Where control features in prolonged gray zone competition, it centers more on activities like the shaping of international technology standards. *Control* features more heavily in war.
- **The relative importance of different domains**, e.g. space versus nuclear or cyber. Compared to the nuclear domain the character of space operations are, for example, more ambiguous and much less destructive (e.g. non-kinetic space operations like dazzling, jamming or spoofing can be reversible). Space is also offense-dominant with no equivalent of second strike mutually assured destruction. This is likely to continue, and thus new technology may change the character of future conflict not only by changing the character of space operations themselves, but also by making space a larger component of any future conflict. Technological advances mean we can anticipate that both space and cyber will play proportionately larger roles for competition in 2031, as described in Parts II and III, and thus the character of these domains will matter more.

Finally, of course, there is a huge amount of path dependence—why did we end up with the "QWERTY" keyboard?—and chance in how technology will change the character of competition for 2031. But we can make educated forecasts based on key drivers of technological change evident now, to which Part II turns.

Part II. Future technologies for 2031



What are the key drivers for technological change ten years from now, in 2031?

We identified key drivers of technological change that suggest the biggest changes in capabilities and impact at scale,[19] based on a review of authoritative horizon scanning efforts and expert discussions[20] – albeit with the caveat that all such efforts will most likely prove only partially correct. Indeed, we chose a timeframe of 10 years ahead to 2031, as that is near enough for sensible predictions yet far enough for significant changes to emerge.

Table 1 summarizes the findings. To avoid repetition, more detailed discussions of aspects of each technology are presented as they arise in Part III.

Six areas emerged. Four of these areas are more traditionally understood areas of technology: software, hardware, biology and space technologies.

Two further key drivers of future technological change are less traditional but will also likely be key.

- First, who will command the technology? We have seen, for example, increasing exertion of Government power over civilian tech companies across the globe—e.g. in the EU, China, India and US—and this will almost certainly increase as new technologies become ever more critical backbones of national infrastructure.
- Second, who will invent and build the technology? China's huge Research and Development (R&D) budget and innovative companies scaling inventions, for example, will very likely continue – and, if so, that must give China more power to set global standards.

Figure 4 illustrates how such less traditional drivers can change: technology mattered in the Cold War and will matter in 2031, but its character will differ.

[19] Two points about the topics chosen: (1) We must also allow for time lags from cutting-edge research: not just from lab to real-world, but also to large-scale in the real-world. The internet, for instance had certainly reached the real-world by the early 1990s—growing up then in London my family had an internet connection—but many of the internet's large-scale real-world impacts took another one decade or two to occur, such as Amazon or Facebook reaching huge scale. (2) We included both higher probability changes (e.g. incremental development and roll out of AI resulting from the leap around 2012) and also lower probability changes (e.g. effective quantum computing that may have a larger impact) as in both cases the expected value (probability multiplied by impact) might be similar.

[20] **Method:** First potential topics were identified through (a) multiple emerging tech or horizon scanning reports (listed below); and (b) discussions with leading technology and innovation experts in the US, UK and EU from within the Government, scholarly and private sectors. This includes ongoing SMA work on emerging technology and innovation. Each of the six areas were then examined in further detail. *Sources reviewed include:* (Defense Science and Technology Laboratory, 2020; Future Today Institute, 2021; Home Office, 2019; NATO Science & Technology Organization, 2020; Office of Communications, 2021; Office of the Director of National Intelligence, 2021). We also reviewed sources such as DARPA's announced priority areas and reports from national academies (e.g. in the US and UK). We reviewed authoritative sources on each of the six areas, e.g. on software (Schmidt et al., 2021), with references cited as they arise in Part III.

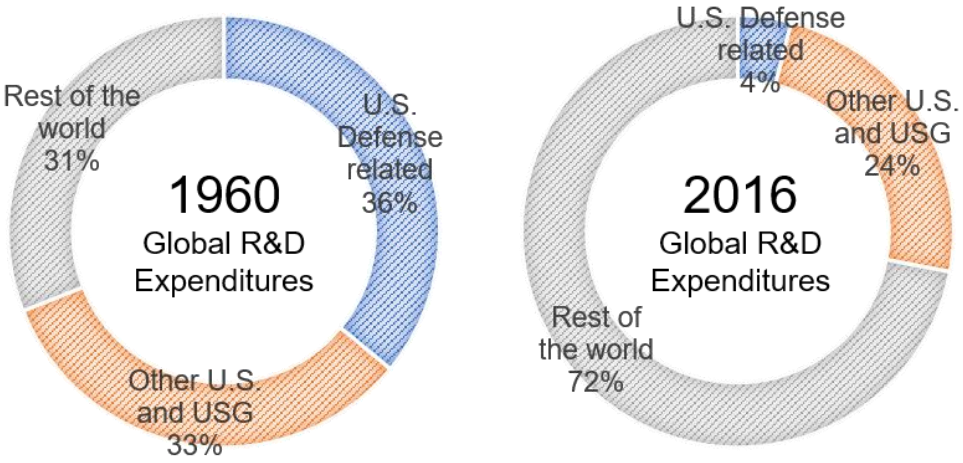


Figure 4 Global R&D expenditures. Source: SMA talk by Mike Brown, Director, Defense Innovation Unit, February 2021.

Software	- AI analysis, often in the cloud, will continue to radically increase the amount of data transformed into information, both about individuals and organizations. - AI will enable new actions by organizations—e.g. vastly complicated military logistics and supply chains—at a scale and pace far beyond current human or bureaucratic capabilities. - Low probability/high impact: AI learning can generalize from small amounts of data, e.g. vastly improving surveillance and enabling machines to operate in unfamiliar environments.
Hardware	- Smarter devices with sensors (e.g. smartphones, “Alexas”, cars, home appliances, in building materials) will enmesh individuals and organizations with greater density (e.g. in the West) and wider coverage (e.g. across Africa). - Global information infrastructure will be rebuilt with new technologies like “5G”, and without forethought by 2031 roll out of “6G” will threaten “Five Eyes” information dominance (Box 6). - Low probability/high impact: Quantum computing may enable (or threaten) decryption of secure traditional communications.
Biology	- Mass-personalization of healthcare for ageing populations (e.g. digitized health records enable new types of research and treatment) plus mass genomics (e.g. large fractions of populations are genotyped) will likely benefit health everywhere. Such information also affords powerful authoritarian tools. - Cheaper and easier dual-use biological weapons tech will lower barriers to entry for small states and non-state actors.
Outer space	- Huge rise in satellite numbers, e.g. after roughly doubling from 2017 to 3,372 now, they are estimated to reach 15,000 by 2028. - Entanglements will increase, such as between “civilian” and “military” space assets (e.g. the US SpaceX; the UK’s “Oneweb”) or between conventional and nuclear missions in space. - Low probability/high impact: Low cost satellite internet access could enable global, tricky to censor internet communications.
Who will command the tech	- Every sovereign entity that can is increasing political control over big tech companies (e.g. the US, China and EU), although methods vary. - Digital sovereignty at the domestic/foreign border is rising everywhere, with a character varying from liberal to authoritarian.
Who will invent and build the tech	- US R&D is now more civilian than military (Figure 4). - China will likely become the world’s largest economy in dollar terms around 2031, and thus likely largest R&D spender. - China will expand its lead in global manufacturing to include more high-tech sectors, unless the US significantly changes policy.

Table 1 Future technology for 2031: Six key areas will drive change.

Part III. Anticipating the future character of information in strategy

What will be the character of information in strategy in 2031?

To tackle this question, we combine information in strategy (Part I) with future technologies (Part II). Anticipating the character of information in strategy is a vast topic beyond the scope of any single report. Thus, here we focus the discussion by considering three scales: populations, great powers and global systems.

US success rests on success at all three scales. Each scale poses distinct, albeit related, challenges. Part III considers each of the three scales in turn, describing key forecasts and making recommendations. It presents likely scenarios and factors in 2031, and so that the reader can better feel themselves in that world in 2031 it uses language such as “x and y will have led to z” – although of course all such forecasts are probabilistic and should be read with that caveat.

We focus mostly on gray zone competition, which is the current situation between the US, China and Russia, and likely to continue over the next few decades. We also discuss war as there is a small but real chance of Sino-US escalation to war, and in particular discuss a long Great Power war as that is an underappreciated risk.

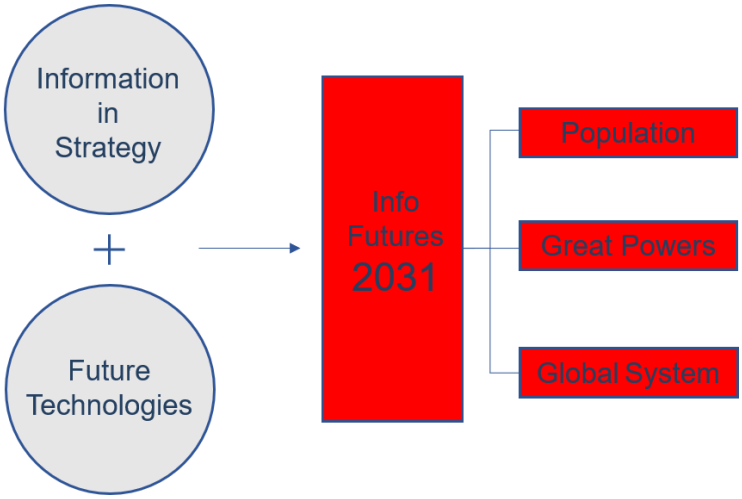
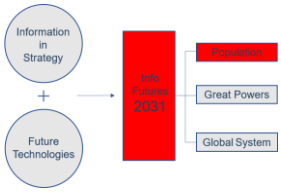


Figure 5 Part III looks at three levels: population, great powers and the global system

Populations in 2031: domestic and foreign information threats



A population, such as that of the United States, faces threats from adversaries and other destabilizing forces that seek to harness information to sow discord, exert influence and obtain information valuable for US security and prosperity. The same is true for the populations of US allies and partners like Japan or Taiwan, as well as in global swing states across Africa, the Middle East, South East Asia and beyond.

A recent Princeton study, for example, described seventy six cases in which foreign governments used social media to influence politics in a range of countries

through propaganda, sowing discord or disinformation (Martin et al., 2020). And, of course, social media is just one of the many ways that information flows through populations, many of which are being leveraged to disrupt and degrade societies.[21]

In 2031, the existence of these threats will not be new. Previous epochs of gray zone competition, like those before World War Two or during the Cold War, also saw such threats (Rid, 2020). But as these threats harness the powerful new technologies immersing our lives, their character will change.

(1) Foreign/domestic information integration: digital boundaries and managed openness

Summary: *Digital tech trends will have made the merger across the boundary between "domestic" and "foreign" information spheres* ***deeper*** *for most populations (e.g. in the US, UK or EU[22]). But countervailing political forces will also make digital boundaries around populations* ***lumpier****, in that the increased integration will be greater in some relationships (e.g. US-Australia) than in others (e.g. US-Russia) and in some sectors (e.g. healthcare) than others. "Managed openness" provides a path forward for the US to defend its population and generate advantages when operating across this deeper and lumpier boundary.*

Thinking encapsulated in the new US Interim National Security Strategic Guidance (INSSG; Biden, 2021) stresses the merger of domestic and foreign policy. But to anticipate the domestic-foreign relationship in 2031 requires anticipating the character of its ever growing digital dimension. In that technological context: what is a boundary and, therefore, what is domestic and foreign?

A boundary is the limit around the edge of something, dividing it from other things. A boundary is crucial for an agent at any scale of human life: indeed, life itself can be defined as order within a border. Boundaries at all scales of human life selectively let things in, such as signals, whilst keeping others out.[23] China, for instance, has been a state, with taxes, administrators and boundaries for much of two millennia – famous for its "Great Wall." Such boundaries are a crucial means by which all states create order in a border.

Over the past two decades, the digital technologies in particular have greatly increased the significance of countries' boundaries that are not just traditional geographical boundaries – the populations in Idaho, Kansas and St Louis now have every day, real-time digital boundaries with China, Russia, Japan and Australia. As Figure 6 depicts, this can be seen as an alternative "geography." Sowing discord in Delaware used to be difficult, but no longer. This is a crucial digital boundary that the US national security apparatus must protect and operate across.

---

[21] A recent series of reports examining these issues is found at https://www.ned.org/sharp-power-and-democratic-resilience-series/.

[22] The EU is not a classic country. The EU's sovereign powers are, however, increasing rapidly and in particular for cyberspace where boundaries relate more to competing regulatory regimes than some other domains. EU exertion of power through regulation is well known, e.g. via "GDPR" in the digital domain, and has been more broadly discussed as "The Brussels Effect" (Bradford, 2020).

[23] Consider a cell's membrane. No mere barrier, this creates order. One third of all energy used by human cells (and thus, roughly, of the last thing you ate) powers a specific membrane pump that pushes the metals sodium and potassium in and out. If that pump ceases, your cell dies (Wolpert, 2010).

Figure 6 Boundaries with new technology. Already in 2021 an increasingly important alternative "geography" means that Idaho, Kansas and Chicago have everyday, real-time digital boundaries with China, Russia, Australia and so on. By 2031, the interactions across this US boundary will be both more integrated (e.g. greater data flows) and lumpier (e.g. US increase in integration greater with Canada than China).

In 2031, we can anticipate a **deeper** and **lumpier** character of the boundary around the US population than seen now. This will result from two major sets of forces.

First are a set of forces towards *deeper* information integration between many populations. In 2031:

- Continued proliferation of digital hardware (e.g. the internet of things), software (e.g. AI for digital assistants), and biological technologies (e.g. health records, genomics and wearable physiological monitors) will have deepened their penetration within almost all populations for data collection and information generation.
- Global economies of scale in the production of these technologies will continue to facilitate their inter-operability across borders. It is hard to compete against an established Google, Facebook, Alibaba or Apple.
- Cloud services provided across borders will also have proliferated further. New services are often built on compatible platforms like Amazon Web Services, which facilitates integration across many (although not all) borders. Recent figures suggest the US stores some 92 percent of the Western world's data (Propp, 2019). Increasing amounts of data processing, not just storage, also occurs in the cloud.
- Space companies like SpaceX or OneWeb may well also enable global satellite data services that are tricky to censor (The Economist, 2021a).

But countervailing political forces will also make digital boundaries around populations *lumpier*, by which we mean that the increased integration will be much greater in some relationships (e.g. US-Australia) than in others (e.g. (US-Russia) and

in some sectors (e.g. social media) than others (e.g. sensitive healthcare data). Such forces relate to the key tech driver from Part II, "who will command the tech" (Table 1). In 2031:

- Authoritarian regimes, notably China, will have continued to develop their digital boundaries against incoming information that they wish to prevent from reaching their population at scale. Vast AI-human systems will enable highly selective censorship, so economically or scientifically productive information will be allowed in. Given the diversity of authoritarian regime types—e.g. China's, those across the Middle East or Russia's "hybrid" democratic-authoritarian model—many options for how to implement **digital authoritarian** boundaries will have emerged for others to copy. At the same time China's efforts to entrench itself in other countries by building much of their digital infrastructure and ecosystem will reinforce the 'lumpiness' of digital boundaries.
- Western liberal democracies like the US will have adopted further measures to protect increasingly digitized critical national infrastructure such as election processes, gas pipelines or food supplies. All countries will have faced a basic set of challenges: how can one draw a boundary around a population in order to defend it (e.g. to defend Australia, New Zealand or Taiwan from Chinese information operations), tax it (e.g. to pay for public services) and police it (e.g. to prevent child pornography)? Again, diverse types of democracies will have provided diverse models for digital boundaries, for instance with the EU likely to have continued to pursue "tech sovereignty" (von der Leyen, 2020) and localizing data within itself (e.g. via its sovereign cloud currently called "Gaia-X"). Diverse models of **democratic digital sovereignty** will emerge.
- Already in 2021, Chicago or Springfield in Illinois, Alpharetta in Georgia (the headquarters of the recently hacked "Colonial Pipeline") and every other US community now have borders with China, Russia, Switzerland, Japan and essentially everywhere else. This includes private companies and individuals who conceive of themselves as far from a boundary. By 2031, both for democracies like the US and authoritarian states like China or Russia, the **whole of society** will present even more of a vast attack surface – requiring new means of protection. What style such protection takes will depend largely on a country's domestic political regime type.
- Lumpiness at the digital boundary will also differ by sector. Consider three broad sectors: (a) entertainment (e.g. video-on-demand like Netflix or Disney) and social media (e.g. Facebook) will remain lumpy[24], but will also be much more integrated across most borders than; (b) medical records, which are a type of data that rightly have special legal protections (e.g. current "HIPAA" rules on digital records in the US); or (c) innovation in

[24] All countries have slightly differing ideas about issues like limits to free speech and public service broadcasting. Not everything goes in the US, as illustrated somewhat inaccurately by the idea that one cannot shout "shouting "Fire!" in a crowded theater". Germany has particular laws on Nazi text. Britain has the BBC. Chinese owned TikTok is already by 2021 accruing vast and valuable data on a large proportion of the US population, and it is entirely possible that action will be taken to stem this data flow at some point.

areas like AI and quantum that directly relate to national security, or increasingly are dual-use, or have significant commercial value (Box 5).

- Lumpiness will also differ between clusters of countries. Groups like the Five Eyes nations have long collaborated on information technologies. The EU, for example, will almost certainly have continued to pursue its ideas of "tech sovereignty", its own rules and processes for data, and digital IDs for all EU citizens (Cater, 2021; European Commission, n.d.).

Thus, the US digital boundary in 2031 will be both more deeply integrated *and* lumpier than it is now. Both matter when considering information operations and other threats against populations, as illustrated in the following ways:

- Deeper integration matters because new methods—human, machine, organizational and legal—will be needed to protect against threats in 2031 when vastly more data flows across a myriad entry points through the domestic-foreign boundary.
- US allies and partners will also face the challenge of deeper integration – and this amplifies a key strategic challenge for the US itself. The US has a strategic asymmetry with China because, unlike the US, China only has North Korea as an ally. Unless US allies and partners can protect their boundaries, US openness to allies will provide more routes into the US population. Additionally, as raised at the June 2021 NATO summit[25], the US must consider how to provide extended defense of these allies if they invoke Article 5 after a cyber-attack.
- "Defending forwards" to protect the US will be crucial in such an increasingly integrated environment—see Box 4—and this must take account of 2031's lumpier terrain both legally and technically. What can be done in and through Five Eyes nations, the EU, India and so on?
- Greater lumpiness also matters because the US benefits hugely from openness (e.g. see Part III's last section on finance and telecoms), and in 2031 such openness will inevitably be more managed. Thus, the US must be ahead of this trend to shape managed openness to the strategic benefit of the US and democracies more broadly – and be a powerful example.

Recommendation III.1. Operationalizing plans like the Interim National Security Strategic Guidance (INSSG; Biden, 2021) to **merge domestic and foreign policy** must anticipate the **deeper and lumpier boundary** between them in 2031. A framework of **"managed openness"** generates advantages from this new terrain, e.g. when defending forward in cyber, or building secure networks with allies to enable the open connections that drive innovation.

- The US should proactively develop "managed openness" of digital boundaries that—as seen with boundaries at every scale of human life from the cell to the individual and the state—requires being neither too open nor too closed. Openness provides huge benefits as it enables the tangled connections between humans and organizations that help

[25] At the June 2021 summit, NATO heads of state and government approved a cyber defence strategy and extended powers to invoke the alliance's Article 5 principle of collective defence in cases of co-ordinated cyber-attacks (Peel & Fedor, 2021).

populations to thrive economically, socially and politically. But such connections also require a foundation of security and trust. Thus, for example, some sensitive networks will always be kept as domestic, and some will only involve alliances long-established to collaborate on the most sensitive topics (e.g. amongst the Five Eyes intelligence-sharing apparatus).

- Importantly, such domestic resilience and deep collaboration does not exclude other networks, but instead lays solid foundations for multiple networks that balance security and the benefits of interchange. They can be considered as concentric circles (Figure 7).
- Whilst this report considers managed openness related to technology, it must also be applied to protect democratic institutions from authoritarian "sharp power" exerted more broadly via media, think tanks, universities and flows of finance.[26] Moreover, as the US increasingly builds mechanisms to defend its digital sovereignty, it must shape global debates by providing a model of democratic digital sovereignty to compete with authoritarian models (Wright, 2020). Finally, managed openness will require action at global scale, as discussed later in Part III.
- Three examples of applying managed openness are:
    - digital defense, including defending forward, in computer network operations (Box 4);
    - information sharing for innovation between populations (Box 5); and
    - cognitive defense of the US Joint Force itself and its support networks, which is the topic of a companion report for this SMA effort, *"Cognitive defense of the Joint Force in a digitizing world"*, available from www.intelligentbiology.co.uk.

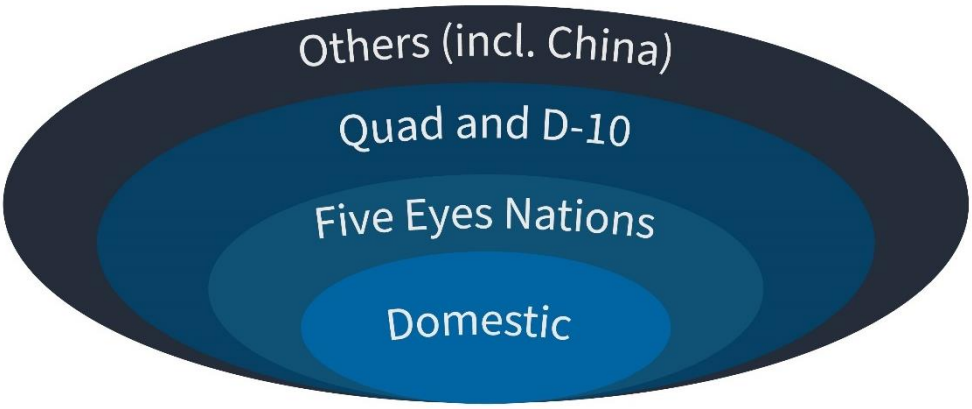


Figure 7 Managed openness networks that balances security and the benefits of interchange. See Boxes 4 and 5 for applications to digital defense and innovation respectively.

[26] A recent series of reports examining these issues is found at https://www.ned.org/sharp-power-and-democratic-resilience-series/.

Box 4. Defending forward across more integrated and lumpier boundaries

US thinking on cyber has been moving towards ideas like "defending forward", "proactive defense" or "persistent engagement" (Nakasone & Sulmeyer, 2021). Indeed, the Cyberspace Solarium Commission (2020) recommended expanding the concept of "defending forward", which originated in the 2018 DoD Cyber Strategy, into a whole-of-government approach involving: "The proactive observing, pursuing, and countering of adversary operations and imposing of costs in day-to-day competition to disrupt and defeat ongoing malicious adversary cyber campaigns, deter future campaigns, and reinforce favorable international norms of behavior, using all of the instruments of national power."

But such ideas face a challenge: how can the US pursue adversaries effectively across the computer networks of allies and partners whilst also respecting their sovereignty and territorial integrity? In 2017, for example, US Cyber Command operators wiped Islamic State propaganda material from a server located in Germany, frustrating the German Government who had received some notification, but not been asked for advance consent (Smeets, 2019). Increasingly, Russian and Chinese hackers use servers based in Western countries, including the US (Volz & McMillan, 2021).

Already a problem in 2021, by 2031 deeper cross-border integration with allies and partners will increase potential routes into the US. Moreover, it is likely that some entities like the EU will have developed greater capabilities to defend their "digital sovereignty", creating lumpier boundaries across which the US will operate.

Current US doctrine does not help grasp this challenge. In Joint Publication 3-12 (2018), *Cyberspace Operations*, allies are essentially part of the "gray cyberspace" (a term not to be confused with "gray zone") that is left over between "blue cyberspace" (areas protected by the US and its mission partners) and "red cyberspace" (areas owned or controlled by an adversary). Further, as Max Smeets (2019) notes, in addition if an adversary (e.g. Russian intelligence) controls a node in an ally (e.g. the Netherlands) then that node may be considered "red cyberspace."

As ever more critical infrastructure within allies digitizes, as allies increasingly care about their own "digital sovereignty" and as allies like the UK move towards active defense themselves – it is unlikely that allies and partners will to continue acquiescing to such US activity without reciprocity that the US is unlikely to desire.

"Managed openness" based around different relationships with different allies and partners is likely to emerge, which the US should proactively shape. As the Solarium Commission suggests, US organizations "should continue and expand efforts with allies and partners to gain permission (when practical) to implement defend forward—e.g. in hunt forward activities, in deceptive countermeasures, for early warning, and providing resources to support hardening defenses." The deepest links will likely build quite straightforwardly on the existing partnership amongst the Five Eyes nations, as noted by the Solarium Commission and even those who foresee problems with "defend forward" (Smeets, 2019). The next circle out, the D-10, will require balancing the political friction with allies from intrusions against vulnerabilities from adversary cyber operations.

Box 5. Innovating with allies: A global edge via managed openness

Cooperation between democratic allies and partners is crucial, and so is the imperative to build science and innovation, but this raises a question: How can democracies practically build science and innovation with allies and partners? China's emergence as a peer-innovator makes this question urgent. Consider the following practical paths forward for the US, UK, Canada, Australia, and New Zealand—the "Five Eyes" nations, not just their intelligence sharing apparatus—in key areas for national security like AI and genetics.

Why now? Deep, tangled connections generate the distributed process of innovation *within* each national innovation system. But innovation at the scale needed now means bringing ecosystems *together* to be more than the sum of the parts. It can greatly enhance even U.S. strength: adding the five nations' global top 100 ranked universities together takes a U.S. tally of 27 to a **far more powerful 56 out of 100**.

Who should **the Five Nations collaborate with?** Domestic resilience and deep collaboration with Five Eyes nations does not exclude other networks, but instead lays solid foundations for multiple networks that balance security and the benefits of interchange. They can be considered as concentric circles.

Strategy for the Five Nations – Managed openness

Managed openness across the five nations can enhance the tangled connections—and minimize barriers—for researchers, investors, and entrepreneurs. Five proposals go from the scientific to the business and global spheres.

Recommendation 1: Organize regular meetings between **all five chief science advisers** (CSAs), as well as key related **government leads** (e.g., emerging tech or manufacturing), in order to coordinate activities and develop these offices in interoperable ways.

Recommendation 2: Create a collaborative, multilateral, truly **five-nation funding scheme for university-led research** (e.g., projects require researchers from at least two nations) in key security or dual-use areas (e.g., AI, space, quantum, genetics) that uses best practice from the five nations as a model of simplicity and speed. National awards will match inputs (i.e., no overall funding of others' jobs).

Recommendation 3: Reduce barriers and enhance infrastructure for firms collaborating across the five nations on the **national security industrial base**. For instance: (a) Adopt more modular procurement (e.g., DARPA's "mosaic" methods to combine small, cheap, flexible systems). (b) Minimize necessary bureaucratic and legal barriers (e.g., replace the many similar MOUs required by the U.S. DOD's branches with overarching multi-nation MOUs).

Recommendation 4: Map the **civilian tech innovation ecosystems** across the five nations in key dual-use and strategic tech (e.g., AI), to identify potentially fruitful links between cities, firms, and clusters in this bigger—and still secure—pool.

Recommendation 5: Leverage this community of five nations to help develop **international tech standards** (e.g., in key standards bodies) and collaborative forms for **extension to other allies and partners** (e.g., Japan, India, Israel, Sweden) and groupings (e.g., NATO, G7, D-10, the Quad).

This Box draws on (Wright, Rees, et al., 2021)*. University ranking data from QS.*

(2) Defending populations in 2031: "3 Ds" and silos as strategic advantage

Summary: *The US population faces threats from adversaries and other destabilizing forces that use information to sow discord, exert influence and obtain valuable knowledge. They will use new tech like AI. Responding effectively to information operations against the US population in 2031 will require new technical, human and organizational capabilities, which are encapsulated by a strategy centered on* ***"3 Ds": Detect, Defend,*** *and* ***Democratic compatibility****.*

In June 2021 China unveiled Wu Dao 2.0, a new AI model. It can understand what people say including their grammar; recognize images and generate realistic pictures based on descriptions; write essays and poems in traditional Chinese; and predict the 3D structures of proteins (Heikkilä, 2021). All these things are hard, but Wu Dao 2.0 is really an advance because it claims to do them all. Its closest rival is GPT-3, developed by the US firm OpenAI and widely held to be the world's best language generator – and in comparison Wu Dao 2.0 is by some measures (e.g. number of parameters) ten times more powerful.

This latest Chinese AI illustrates a number of likely points about 2031.

- AI made a big leap around 2012 and we are still largely mining that technological vein. To be sure, another big leap is possible by 2031 that overcomes AI's current limitations (described in Box 7), but that leap is less likely as one must bear in mind it took decades to get from the consolidation of "deep learning" methods in the 1980s to the big leap deep learning enabled around 2012.
- The race to build cutting edge machines of gigantic size is now largely between the US and China, and this dominance looks more likely to continue than not.[27] To be sure, US allies provide a crucial edge. Google's pioneering DeepMind, for instance, remains near the London lab it was spun out from, the same lab at which AI pioneer Geffrey Hinton worked before moving to Canada where he was the senior author on the 2012 "deep learning" work that sparked AI's current explosion (Krizhevsky et al., 2012). But US allies alone don't have the same heft. The EU is currently far behind.
- Wu Dao 2.0 is cutting edge research, and by 2031 we can anticipate likely widespread commercial use of such capabilities. Companies like Google are betting on such models as a way to revolutionize online search, opening the way for a future in which consumers could ask their devices anything, and obtain responses that seem to be written by an expert (Heikkilä, 2021).
- This is dual use technology, and we can anticipate it will be adapted for information operations against populations, even if some of the capabilities are held in reserve to use in only the most serious contingencies like war.

[27] The Economist, for instance, recently described how America and, increasingly, China are ascendant, accounting for 76 of the world's 100 most valuable firms. Meanwhile, Europe's tally has fallen from 41 in 2000 to 15 today. The pipeline of next global giants looked set to continue this trend (The Economist, 2021b).

- Finally, while both DeepMind and OpenAI are in the private sector, Wu Dao 2.0 is more closely linked to and funded by the Chinese Government.

The companion report for this SMA project, entitled *"Cognitive defense of the Joint Force in a digitizing world"*[28], provides a more detailed breakdown and definition of the character of information operations that the US population will face. While that report focusses on the US Joint Force—which has particular features—the challenge's basic outline is the same. A population, such as that of the United States, faces threats from adversaries and other destabilizing forces that seek to harness information to sow discord, exert influence and obtain information valuable for US security and prosperity.

The evolving character of these threats to the US population are illustrated by "deepfakes."[29] Deepfakes have been around since around 2017, and are AI-generated synthetic media (e.g. images, video or audio) that most commonly involve a person saying or doing something that they did not say or do. Deepfakes can be tools of mass-produced disinformation, or of exquisite "active measures." But deepfakes used alone exert limited influence and they require creative humans to generate impacts in target audiences. Moreover, they will likely be most effectively used as one tool in "combined arms" information operations alongside other dual-use tech like micro-targeting, which is a form of online targeted advertising that can employ AI to analyze personal data and identify particular audiences or interests (discussed in Wright 2021b).

Wu Dao 2.0's great, great, great, AI grandchildren in 2031 will have far greater faking capabilities than a 2021 deepfake-generator, but will still very likely require harnessing as part of a "combined arms" information effort. And Wu Dao 2.0's powerful descendants will be able to help with those other arms, including in the acquisition (e.g. via hacking) and effective deployment of personally embarrassing information. In 2031, AI will routinely tailor advertising or medical treatments to individuals, and in the same way will AI enable the **mass personalization of information operations at population scale** (described in Box 3 of the companion report Wright 2021b, "*Cognitive defense of the Joint Force in a digitizing world"*).

In 2031 data to train these AI models will likely remain key, and how well the US defends its data over the next decade will determine a key a question – will the data on the US population accumulated by adversaries up to 2031 be a relative strategic strength or a weakness for the US? The integration of data is critical, particularly when it includes the incredibly valuable "ground truth" data (e.g. tax returns) that often only governments have or heavily regulate (e.g. medical records or genetic data), because such "ground truth" data can act like labels to train AI on broader data from sources like smartphones or social media usage (Box 7). This raises two implications for US defense of its population in 2031:

- Firstly, the US political system may **give the US a big strategic advantage** compared to China – but one that is often overlooked, and one that requires seizing by US domestic policy. One of the most effective ways to prevent an adversary from acquiring large amounts of data about individuals is to "silo" different sources of data about them (Wright, 2020).

[28] Download from www.intelligentbiology.co.uk.
[29] Deepfakes are discussed at more length in the companion report, *"Cognitive defense of the Joint Force in a digitizing world"* (Wright, 2021b) www.intelligentbiology.co.uk.

But while siloing is possible for the US—and, indeed, is often the status quo—by contrast China is actively building vast "data lakes" of unsiloed, powerful data because their political system requires them to conduct continual, large-scale domestic information operations. To be sure, creating or preserving silos requires a trade-off because some data-sharing brings efficiencies and "breaking silos" is the dogma amongst many leading voices not least when funded by big tech. But crucially there is a trade-off. The disastrous Chinese hack removing intimate data about 22 million security-cleared employees from the US Office of Personnel Management illustrates an inherent problem of building a giant, irresistibly rich target (Perera, 2015; Sanger, 2018). China aims to build data lakes across its vast population, which will inevitably be hard to protect. China's Social Credit System is an example (Wright, 2019b).

- Hardware also matters. "6G", for example, will likely be readying for roll out by 2030 – and if China determines the standards for building 6G this may build in risks of data exfiltration from individuals or organizations across the US population (Box 6). More broadly, digital things—Alexas, toasters, cars, lights, office furniture, medical equipment—will penetrate everywhere in our lives even more deeply in 2031, and it matters profoundly whether they: (a) have privacy baked into their design and defaults; or (b) form an open and integrated book for total public or private surveillance. Many experts argue authoritarian governments tried to embed the latter into standards for the "internet of things" at the UN's International Telecommunication Union (ITU), through a "Digital Object Architecture" scheme that would have assigned each digital object a unique, persistent, government-registered identifier (Chen et al., 2018; Exeter University, n.d.; Lazanki, n.d.). Similar debates surround facial recognition, video monitoring, city and vehicle surveillance (Murgia et al., 2019).

Put simply, the US is now making choices about the character of the information terrain on which it will have to defend its population in 2031. And a successful defense of the US population is to react effectively to adversarial threats, within the constraints of a free society.

Recommendation III.2. Responding effectively to information threats to the US population will require new human, technical and organizational capabilities. These are captured by a strategy built on "**3 Ds**": **Detect, Defend**, and **Democratic compatibility**. All three D's are necessary, and none is sufficient.

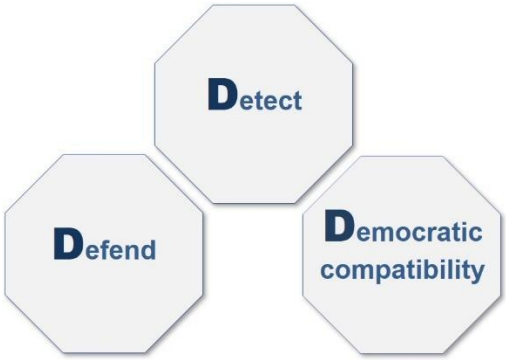


Figure 8 "3D's" of strategy to defend the US population against information threats in 2031.

These three principles are discussed at greater length in the companion publication for this SMA effort: Wright (2021b) *"Cognitive defense of the Joint Force in a digitizing world"* (download from www.intelligentbiology.co.uk). A summary is included below.

DETECT: The US must build capabilities to detect and characterize adversary influence operations – who is targeted, by what means and for what purposes? They must work at multiple scales, which includes:

- detecting specific fakes generated by future versions of Wu Dao 2.0;
- detecting big coordinated campaigns; and
- detecting how others shape the terrain over years, such as understanding how TikTok determines what target audiences in the US see.

DEFEND: Human cognition will always contain vulnerabilities as targets for disruption, as we often respond to grievances, fears and other human motivations. Individuals must also be given the technological means to defend themselves online, for which low cost, practical options exist. But the individual scale is not enough.

Mass personalization of influence operations is coming (as already seen for retail and healthcare) in which personal data will be a key weapon (e.g. combining detailed data from medical records and broader data from TikTok use) and these data on US populations must be better protected.

Silos for data on the US population can be a key US advantage over China for 2031, for example, because China is making itself vulnerable by constructing vast databases for authoritarian control (Wright, 2019b).

New human-AI teams and organization are also needed at the scale of this defensive challenge, which must harness "combined arms" information operations that bring together the latest technological advances with human creatives and adaptable organizational structures. These must harness the key features of information discussed in Box 2 in Part I (e.g. surprise) and anticipate how they will matter for these new tools.

DEMOCRATIC COMPATIBILITY: New capabilities must be placed within ethical, legal and political frameworks that render them compatible with a free society. The military must maintain Posse Comitatus and intelligence oversight, whilst also mitigating the gaps and lack of agility they entail. US Restraint is not a bug, and is instead a key strength of the US system – as it was during the Cold War (Rid, 2020) and will be in 2031.

Box 6. 6G: Sixth generation cellular network infrastructure

Sets of technical rules define how each generation of telecommunications networks operates. This includes which radio frequencies are used to communicate information and how information is ferried by components like cellular devices, antennae and base stations (Gorman, 2020). Since the first handheld mobile phone call in 1973, stepping through the generations helps see how 6G will likely to fit in.

1G: *Analog voice*. New "cellular" networks were built in the late 1970s and 1980s.

2G: *Digital voice and basic data*. Built in the 1990s, 2G networks saw mass consumer adoption. Upgrades included text (SMS), email, and picture messages.

3G: *Smartphones*. The International Telecommunications Union (ITU)'s IMT-2000 standard codified 3G. More bandwidth enabled a smartphone revolution.

4G LTE: *Mobile Broadband*. The 2010s era of true mobile broadband saw large increases in data capacity supporting richer content and connections.

5G: *Connecting the internet of things*. 5G uses faster speeds (10 to 100 times the speed of 4G), higher bandwidth, and lower latency (the lag time in communications between devices and servers). This allows the near-instantaneous communication needed for applications like self-driving cars. It will generate new business models as vast numbers of devices interconnect across homes, businesses and cities.

Who leads in 5G now? The Third Generation Partnership Project (3GPP) is the overarching technical body for proposing global communications standards. Although designed as technocratic, companies benefit if their patents become global standards. As of Feb 2021 China's Huawei led in 3GPP 5G patents: Huawei 15.4%, Samsung 13.3%, Nokia 13.2%, Qualcomm 12.9%, LG 8.7%, ZTE 5.6%, Sharp 4.6% and Erikson 4.6% (IPlytics, 2021). Further, the US alone cannot compete with China in 5G hardware: the US has no large cellular infrastructure provider of the base stations, routers or switches made by Huawei, Ericsson, Nokia, Samsung and ZTE. Crucial in the developing world, Huawei also beats non-Chinese suppliers on cost.

"Open-RAN" is a standard to avoid proprietary software in such systems, and thus depending on suppliers like Huawei. The UK's Vodafone recently turned to Japanese and US companies for Europe's first commercial Open-RAN network (Fildes, 2021).

6G: *Even Faster.* Although scientific obstacles abound, 6G is anticipated to roll out around 2030, with the vision currently for peak download speeds of 1 million Mbps (versus 5G's 10,000 Mbps) and latency of of 0.1 millisecond (versus 5G's 1 millisecond). Super high frequency terahertz waves may achieve that, although no chips are yet capable of transmitting such data. 6G could deliver real-time holograms and far more densely interconnected brains, bodies and environments than 5G.

Can the US regain lost ground with 6G? China started research in 2018, launched a 6G satellite in November 2020 and plans to introduce 6G around 2029 (Zhao et al., 2021). China outnumbers the US alone at the 3PGG and greatly influences the ITU (Gorman, 2020). The US began research in 2018, opened spectrum for experiments, corralled an industry initiative (e.g. with Apple and AT&T) and agreed a 2021 US-Japan investment in Open-RAN and 6G (Nikkei Asia, 2021). The UK, Russia, Japan, South Korea and EU all have 6G efforts (Zhao et al., 2021).

6G will arrive in some form. The US will lose—and cannot win—unless it improves its own game and harnesses alliances for innovation (Box 5).

For a good summary see (Gorman, 2020) on which the 1G-5G descriptions above are based.

Box 7. AI – strengths, weaknesses and human-machine teams

The AI-related technologies comprise the cutting edge of the broader digital technologies. By the term "AI" here I refer to a constellation of AI-related technologies that together provide powerful, wide-ranging and new capabilities: AI more tightly defined, machine learning, big data, and digital things (e.g. the "internet of things"). Together they enable a new industrial revolution, taking the vast reams of data produced by the computers and internet – and turning it into useful information. None is entirely new, but recent big improvements (particularly from "deep learning" around 2012) mean together they have revolutionary applications.

However, these advances have not been uniform, and we must understand two key strengths and two key limitations. **AI is currently good at two things:**

(1) **Perception**, e.g. perceiving images or speech, or some patterns in big data.

(2) AI also improved when choosing actions in **tasks that are bounded enough** to be very well described by vast amounts of (often labelled) data, e.g. logistics in a warehouse.

Thus, real-world impacts now relate largely to perception (e.g. perceiving faces or speech) or some bounded decision tasks (e.g. logistics). Continued rollout in these areas will likely dominate in 2031, and are this report's focus.

But **AI's two key current limitations**, have meant that rolling AI out in the real world, let alone at scale, has proven very tough in many fields (e.g. medicine despite all the hype). These are:

(1) AI deals badly with **context**, so humans are often needed to make even common-sense judgements.

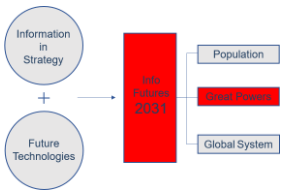
(2) AI requires **huge amounts of often labelled data**, so that setting up datasets is often a crucial precondition.

Thus, because of AI's current limitations it requires extensive human involvement to help deal with context (i.e. **human-machine teams** rather than AI alone); and current efforts will likely try to **acquire large amounts of data** that includes both broad data (e.g. via TikTok) as well as "ground truth" data to act as labels (e.g. medical or financial data via US tech companies, data brokers or espionage).

Low probability but high impact AI advance: If AI research overcomes the problems of context or of requiring large amounts of data—currently very tough problems to crack—then AI's capabilities and impacts will require a big re-assessment. This would, for example, vastly improve surveillance and enable machines to operate in unfamiliar environments.

An analogy is the leap from steam to the internal combustion engine. Steam engines changed the world, but required more bounded environments like a railroad. Internal combustion engines were more versatile, allowing huge advances like the tractor that radically changed farm output.

Great Powers and Superpowers in 2031: information in China-US escalation scenarios and war



A very different type of information challenge arises when considering how large, modern states like the US and USSR signaled information to each other during the 1962 Cuban missile crisis, or how the European powers signaled to each other in the run up to the First and Second World Wars. Compared to the previous section on populations, research on such great power interactions often uses different historical cases and fields of scholarship such as "international relations." Here we consider how technology may affect the character of such competition.

Of course, strategy remains fundamentally human and deep links exist between information in strategy for populations and for great power signaling – so that key features of information, such as surprise, matter in both arenas. Scholar Michael Handel's book "*The Diplomacy of Surprise*" (Handel, 1981), for example, traces the role of surprise in various cases: Adolf Hitler's diplomacy in the years leading up to World War Two; US President Richard Nixon's "opening" to China in 1971; and Egyptian leader Anwar Sadat's use of surprise, including in his peace initiatives and his surprise 1977 speech in the Israeli Knesset. Handel shows how surprise can be a tool to build peace or defeat opponents. Harnessing surprise and predictability to cause intended, and avoid unintended, effects will be key for any future China-US escalation scenario or war.

The US and China will almost certainly be powerful states in 2031.[30] In this section we consider two important ways they may interact: first looking at signaling in escalation scenarios; and then considering the role of information in a long great power war.

(3) Signaling in escalation scenarios: more true and false information, but wisdom?

Summary: *Signaling information between great powers during crises will change, which if unanticipated may cause inadvertent escalation. China will, for example, increasingly see US threats to its digital authoritarian systems (e.g. for "social credit") as threats against regime stability, which the US may poorly understand. The character of "fog" and escalation thresholds will change. More broadly, AI will bring vastly more true and false information, but little enhanced wisdom. Enhanced US capabilities for knowledge and wisdom—operationalized to harness vastly more data and information—could form a crucial US edge.*

[30] A superpower by definition has global reach, and is essentially a great power on every continent, or a 'global great power.' The US is the only current superpower, although China is likely to become one in the next couple of decades. A Great Power is a state deemed to rank amongst the most powerful in a hierarchal state-system, and so capable of holding its own against any other nation (e.g. currently China, Russia, Japan, Gemany, Britain, France). For a discussion see pp35-36 of Wright 2019, v2, *Global Strategy amidst the globe's cultures: Cultures in individual cognition, states and the global system*. www.intelligentbiology.co.uk, for discussion.

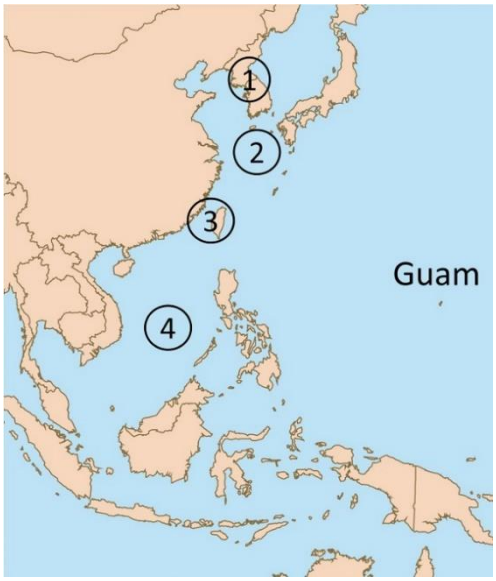


Figure 9. Four potential locations for Sino-U.S. escalation to war. From north to south these are: (1) Korean peninsula; (2) East China Sea; (3) Taiwan; and (4) South China Sea.

Great powers, like the USSR and US during the Cuban missile crisis, send each other signals to communicate information. Signals might be actions like moving ships or mobilizing troops, or messages such as a speech or diplomatic note.

Signaling relates to *influence* rather than control. Both deterrence and escalation management are examples of such influence. As with all types of influence, the fundamentally cognitive dimension of deterrence and escalation management underlies their consistent nature – but their character changes. [31]

This subsection considers China-US escalation scenarios and asks: What will be the most significant differences about the character of signaling in 2031?

Changed character of "fog" in 2031: Carl von Clausewitz wrote that "*War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty."* (Clausewitz, 2008, p. 46). In 2031 the US, China and US allies like Japan will perceive the world through more layers of technology. More hardware sensors and surveillance will produce more data, and then more AI will help turn that into more information. And that information can be good or bad.

- More "good information": Signaling will occur in 2031 with the US and China seeing each other through surveillance machineries that collect much more information, more granular information and new types of information. Dedicated military and intelligence surveillance will expand, e.g. via space and drones. Dual use information will also expand, with an analogy being the "high frequency" information used to understand Covid-19's economic impacts. That Covid-19 information used mobile phone mobility indices, energy use and other alternative indicators to provide a picture of economic and social activity in different countries – which may have been ahead of more standard statistics (Arnold & Romei, 2021; Romei & Burn-Murdoch, 2020). In another analogy, Chinese financial credit-scoring apps have made lending decisions based

[31] For a discussion see Chapter 2 of the SMA report: Wright (2019) v2 *Mindspace: Cognition in Space Operations*. www.intelligentbiology.co.uk

partly on the way users charged their cell phone batteries (Lee, 2018). How should US analysts and decision-makers rely on each new source of information, weight various sources compared to each other, integrate them or consider how their usefulness may change according to context?

- More "bad" information: Both sides in 2031 will also employ clever deception in an attempt to fool the adversary's AI. As Part I described, clever "edge cases" might exploit the AI's programming; or exploit the limitations of the adversary AI's training datasets (because all datasets have limitations); or exploit deficiencies in an adversary's AI deliberately prepared ahead of time (e.g. by feeding it poisoned training data). Is that really an enemy installation hidden inside a hospital, or is that a clever fake to mislead an AI and so induce a politically disastrous misstep? Many powerful exploits will be held back for such serious contingencies to provide so-called "zero day" exploits.[32]

Essentially, AI provides more layers in the process of the great power's "perception" into which deception can be inserted: information has gone from the eye, to the telescope, to the radar, through different layers of thinking in bureaucracies – and now also through AI.[33] And AI's processing is often impossible to meaningfully explain anyway, let alone in the cauldron of a Sino-US escalation scenario.[34]

Managing this new character of the "fog" though which great powers will perceive each other's' signals requires updated machine, human and organizational means to analyze and integrate this information. Ultimately it will all need to go up to the highest level military and then civilian decision-makers (e.g. top US and Chinese politicians) who must interpret information, integrate information and make decisions. Hence the requirement to aim for superiority in data and information – and also knowledge and wisdom.

Changed character of "thresholds" in 2031: AI will also likely change escalation thresholds against which actions are judged – and if not anticipated these changes may cause inadvertent escalation.[35] Consider five examples:

- *Changes to what the other side values in 2031.* Regime security is often held to be the Chinese leadership's primary motivation - and AI will almost certainly change the character of perceived threats to regime stability, as the regime increasingly depends on vast digital systems of social governance. Attacks on that system may be perceived as threats to the regime. What would happen in a crisis 10 years hence if then crucial social governance systems in a major

[32] A vulnerability previously unidentified by the defender so that they have zero days of notice to fix it before damage is done.
[33] Scholar Jon Lindsay makes a similar point in discussion of AI, where "The means of reducing uncertainty, ironically enough, have become new sources of uncertainty" (Goldfarb & Lindsay, 2020). That is, information and communication technologies increase complexity, introduce potential technical errors and security concerns, create challenges managing data and so on, so their effect isn't to eliminate the fog of war but to shift it to the domain of managing these systems. I thank Wyatt Hoffman for making this connection.
[34] "Explainable AI" is a challenge. Deep learning involves the "hidden layers" between inputs and outputs to learn. But how can we explain what those numbers mean in words or concepts that humans can grasp, and how can we do that in a timely fashion? Wu Dao 2.0, described above, reportedly has 1.75 trillion parameters.
[35] For an excellent discussion of thresholds in escalation see (F. E. Morgan et al., 2008).

city such as Chongqing were essentially turned off? To be sure the US political system has potential vulnerabilities, but the profound Chinese vulnerability will be a potentially destabilizing asymmetry in a Sino-US escalation scenario.

- *Changes to what cyber intrusions mean in 2031.* A scramble to gain access to each other's' computer systems, including AI, may be triggered during escalation, but how would this be perceived (Hoffman, 2021)? Such access could intend to provide situational awareness and that could, in principle, even help stabilize a crisis by reassuring the hacker that no first strike was being prepared (analogous to satellite monitoring for signs of nuclear activity). But such access is also dual use and could be used for offensive purposes. As with spiraling mobilizations before World War One, could both sides' intrusions spiral towards war?
- *Changes to the relative importance of domains in 2031.* Cyber and space will likely be more prominent, and signaling in both these domains is often highly ambiguous. Chinese ideas about space operations also differ from those of the US, for instance seeing them as less escalatory. For discussion see Wright (2019), v2, *Mindspace: cognition and space operations* (www.intelligentbiology.co.uk).
- *Changes to how entangled assets are in 2031*. Commercial and military entanglement will increasingly complicate escalation scenarios, for instance with commercial space systems having dual use capabilities. What would it mean if China interfered with the US SpaceX Starlink communication constellation, or the OneWeb constellation that now has UK Government involvement? Digital infrastructure is often commercial rather than Government owned, but can still be critical.
- *Changes to the offense-defense balance – a big unknown.* How AI may affect the offense-defense balance is currently unknown, despite useful analyses on the question (Hoffman, 2021). Previous eras have got this disastrously wrong, such as the widespread thinking before World War One that offense was dominant. Perceptions that offense is dominant and that weapons are vulnerable or their command, control or communication are fragile will create concerns that one must "use it or lose it." (F. E. Morgan et al., 2008, p. 41)
- *Changes to decryption of secret communications from quantum – another big unknown.* Signals intelligence (SIGINT) shaped twentieth century competition from the World Wars to the Cold War (Andrew, 2004), because one must always ask: what are "they" really thinking and what are their intentions? Secure communications within a country, with allies and with an adversary also matter deeply: consider if US-Soviet communications during the Cuban missile crisis had been publicized. Weaponized leaks can be effective, as we have seen over the past two decades (Rid, 2020). A small chance exists that quantum computing will have radically changed signals intelligence by 2031, by vastly reducing the time needed to unlock an encryption scheme (Cyberspace Solarium Commission, 2020, p. 121). Even the looming threat of decryption soon after 2031 may alter behaviors before it becomes available. A period of intense disruption for SIGINT will inject further uncertainty and ambiguity into escalation scenarios.

In addition to the challenges posed by the changes in themselves – if such changes to thresholds are understood differently in China, Russia, and the US, this might also cause misperceptions. Thus, these powers must think through and, where possible, discuss such changes in Track 2 or other dialogues. The urgency of such discussions is illustrated by recent experience with more traditional "cyber" technologies: even basic concepts from the key technologies associated with cyberspace were understood differently (Giles & Hagestad, 2013).

Recommendation III.3a. Anticipate the character of deterrence and escalation management in 2031, as the **character of "fog" and thresholds changes**.

- In addition to the factors described above, an example of such an approach is a recent SMA report that considered the character of influence (e.g. deterrence and escalation management) in space operations: Wright (2019), v2, *Mindspace: cognition and space operations*, available at www.intelligentbiology.co.uk.

Recommendation III.3b. Enhance US capabilities for **knowledge** and **wisdom** – operationalized to harness vastly more **data** and **information**.

- Box 3 in this report describes practical methods, such as net assessment.

(4) Plan for "Day 100" and remember "Day 2193" of a great power war

Summary: *Great power wars often last years or decades. This is not unlikely to recur if a limited China-US conflict broke out, even in our nuclear age, with profound repercussions for the US use of information. The US should explicitly* ***plan for eventualities at Day 100 and beyond****, not least because by the time a war erupts it may be* ***too late*** *to create much of what is needed to win.*

Humans tend to be optimistic, and an often ignored contingency is that a great power war, even in our nuclear age, will not end quickly as we might hope but will instead go for many years – as initially limited wars have so often before.[36] Would the US just give up after an initial reverse in a limited war? Or, instead, facing the choice on Day 100 after many lives had been sacrificed, would the US decide to carry on? Carrying on would fit better with the aim of preventing adversaries from becoming a dangerous hegemon (Walt, 2020), the strategy Britain pursued in Europe for a quarter millennium and the US has pursued globally for much of the time since. Of course, this is not to say a prolonged great power war is likely, but rather that if a limited China-US war erupted then a long war it is not unlikely.

[36] Humans tend to make optimistic assessments across many aspects of life, including of their own abilities, the risks they run with diseases, and their planning for projects (Sharot et al., 2011). Indeed, the UK Government introduced a correction for this "optimism bias" into their official Whitehall guidelines for project planning (HM Treasury, 2018). Optimistic assessments are suggested as a cause of war (Johnson & Tierney, 2011). Prominent voices before the First and Second World Wars decried the slaughter that would occur with industrial scale weapons, and yet they occurred. Moreover, while nuclear weapons clearly make any such war more dangerous, although we now know how close the Cold War came to nuclear use, e.g. during the Cuban Missile Crisis in 1962 or the Able Archer exercise in 1983.

Thus, think ahead a little to “Day 100”, and indeed to “Day 2193” that was how long World War Two lasted for Britain from 1939 to 1945. Lack of planning for unwelcome contingencies has hurt the US recently, as seen with Iraq in 2003.

So, what will be the character of information for strategy in a prolonged great power war? Much of how any prolonged war will develop is unknowable, but here I begin by asking four questions for 2031.

- *What will be the character of US reserve capabilities—and thus ability to rise to the challenge of a long war—in 2031?* In all of 1939 the US built only six medium tanks (Gruber & Johnson, 2019), but it ended World War Two manufacturing at vast scale. The US had a large civilian industrial base that it could bring to bear. What will be the situation in 2031 for key technological areas: software, hardware, biological and space? Unless trajectories significantly alter[37], the US will continue to have large reserves of capabilities in software, biology and space but will be significantly challenged in hardware relative to China. Whether the US would be able, during a war, to build the new manufacturing capacity to compete with China is unclear. And what if the US sought to buy goods at scale from third parties? Even if third parties could supply the goods, if the key third party were a single actor unlikely to be involved militarily early on—like the EU—that would risk a vast transfer of wealth analogous to Britain’s wealth transfer to the US in both World Wars.

  Getting ahead of this challenge requires the US to build up **robust, diversified manufacturing supply chains**, which as Covid-19 showed also brings broader benefits. It can involve various groupings like the Five Eyes community of nations (members of which are also likely to be militarily involved), and the broader “Democratic-10” or “D-10” (Box 5).[38]
- *What will be the character of a long war involving AI and cyber in 2031?* Clearly tactical level use of cyber will be a routine and a valuable tool – but what about cyber’s strategic effects on domestic industrial production? Large, industrial states under basically competent leadership can absorb vast and prolonged strategic attacks without collapse, such as strategic bombing of Britain and of Germany in World War Two. As scholar Jim Lewis wrote “The effect of attacks on infrastructure is easy to overestimate. Cyber-attacks will resemble those actions where guerrillas blow up substations or pull down power pylons to remind the opposing government that they are there and to erode its legitimacy.” (Lewis, 2010) Power disruptions can be managed, for instance, as Texas recently showed

[37] At the time of writing the US and China both have good pipelines of up and coming companies (The Economist, 2021b). But in hardware China is the world’s manufacturing superpower with 28.4% of global manufacturing output in 2018, which is similar to the next three countries combined: US 16.6%, Japan 7.2% and Germany 5.8%. Consider the specific case of semiconductors. The number of manufacturers at that industry’s cutting-edge has fallen from over 25 in 2000 to three—Intel, Samsung and Taiwan’s TSMC—of which Intel is seriously falling behind (Economist, 2021b). The Semiconductor Industry Association, an American trade body, reckons that 80% of global chipmaking capacity now resides in Asia. China has put semiconductors at the core of a multibillion-dollar plan to become self-sufficient in critical technologies by 2025—especially now that American sanctions have deprived it of some foreign imports (Economist, 2021a).

[38] For a discussion of supply chains and the example of the biological technologies, see (Wright, Giordano, et al., 2021).

following adverse weather, and would unlikely be worse with cyber than the World War Two strategic bombing that brought neither Britain nor Germany to its knees.

Building **resilience and siloing digital systems** will be key. An example is separating the front and back office parts of infrastructure like the recently hacked "Colonial Pipeline".

- *What will be the character of a long war with AI-enabled Precision Guided Munitions in 2031?* AI is good at surveillance and making decisions within constrained contexts (Box 7), which may together render the seas around the battlespace extremely inhospitable for ships or aircraft from either side. Many hundreds of miles of sea around Taiwan, for instance, may become analogous to the blasted no man's land between trenches in World War One.

  Such defense dominance is at least plausible. In such struggles, key issues include not losing too badly in the initial phase of the conflict, and having the manufacturing capacity to replace munitions (Dougherty, 2014).

- *What will be the character of a long war with space operations in 2031?* The Chinese space industrial and scientific complex will still likely lag behind the U.S., although the gap will have narrowed. Indeed by 2031 China may sufficiently large space dependencies in a Sino-U.S. Taiwan escalation scenario that it really feels it has "something to lose" in space (Wright, 2019, *Mindspace*, Chapter 6, p. 65). Thus, China may not resort to early, large-scale kinetic space operations. However, space operations will remain ambiguous and will have become much more congested. Moreover, long wars over years can change strategic calculi, an example being First World War German restraint in U-boat warfare from 1914 and eventual 1917 adoption of unrestricted U-boat warfare – and this may bring Chinese ideas such as "space blockade" using debris more into the realm of the possible.

  Space will remain dangerous as there may still be a major risk of "entanglement" between the US nuclear and conventional missions in space in 2031, particularly if the replacement of the US dual-use SBIRs satellites[39] is with a similar small constellation of exquisite assets rather than a more resilient system in other orbits.[40] More resilient space systems and redundancy via non-space systems, where possible, will remain key even as the US and China move towards a potentially more stable parity of space dependency.

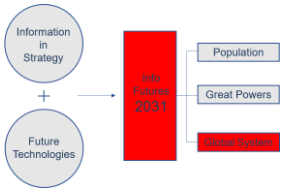
Recommendation III.4a. Recognize that long wars happen between great powers and explicitly plan for eventualities at Day 100 and beyond.

- What may seem unthinkable before Day 1 may look very different on Day 100 in light of sunk costs, human casualties and emotions on all sides.

[39] They have a role detecting launches of both nuclear and conventional missiles (Acton, 2018).
[40] Based on public announcements the plans are unclear, but while DoD leaders have discussed other orbits (Hitchens, 2020) other reports call that enhanced resilience into question (*Future Defense Spending*, 2021).

Recommendation *III.4b.* By the time a war erupts it may be **too late** to create much of what is needed for a long war. Thus, anticipate key needs for a long war, and also build critical systems for resilience not just maximum efficiency.

Global information systems in 2031: global strategy for global competition



The globe is vast, with some 193 countries, 4.66 billion internet users and 7000 languages. TikTok alone has 689 million active users outside China (Sehl, 2021). In 2020, global internet traffic was estimated to be more than 3 zettabytes, or 3,000,000,000,000 gigabytes, which is equivalent to 325 million households watching Netflix simultaneously every minute of the day – and that is set to increase by 50% by 2022, let alone 2031 (World Bank, 2021).

So, how can the US make "global strategy" with information? This matters: the US shaped global systems for information more than any other power since 1945, and these systems—from telecoms to finance—have hugely benefited the US and much of the globe. Whoever leads the global system's next epoch will accrue those benefits – and make the world more or less free.

Global strategy involves important activities and interests in all the continents that contain a significant fraction of the world's population. It isn't just grand strategy, which any state can have. It isn't just international strategy: the global system differs from the sum of its nations, because of transnational societal networks and domains like global finance or cyber (Box 8). Three of the conflicts that have defined the US were global: the two World Wars and the Cold War. A previous SMA project[41] examined global strategy and two key recommendations were:

- **Adopt a global mindset**. Policymaking should include a global vantage point.
- **Use global system effects, not just actor-specific effects.** The US may most decisively influence China, for instance, via actions through global financial systems. But in 2031, will the US retain its centrality in global financial information flows?

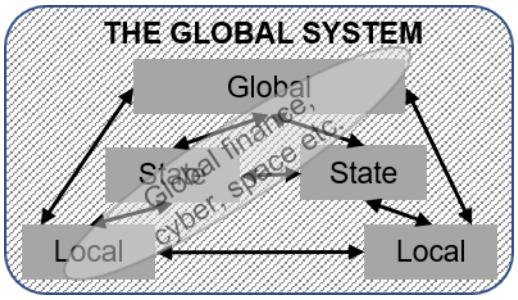
In this final section we explore an example: how the US can generate power from its centrality in global information flows.

[41] Wright, 2019, v2, *Global Strategy amidst the globe's cultures: Cultures in individual cognition, states and the global system*. www.intelligentbiology.co.uk.

Box 8. The global system

The **global system** is a system-of-systems covering the whole of human society across all the world's continents on which significant fractions of the world's population live, and its key sub-systems include:

- states (e.g. the US or China),
- highly globalized subsystems (e.g. the global financial system or the UN), and
- systems at other scales (e.g. sub-state regions like Catalonia; or above the state like the competing Cold War liberal and Communist international systems).



The global system isn't a thin crust sitting atop billiard-ball-like states[42] – it is the system-of-systems *incorporating* all the way from the global down to the local scale and to human individuals. States are themselves systems-of-systems. But although states like China or the US remain key, other subsystems are currently so globalized (i.e. driven by factors at the global rather than lower scales) that understanding them requires an at least partly global perspective. Examples include:

Global financial system: The global scale of finance is shown by the worldwide effects of financial crises like those in 2007-9 or the interwar 'Great Depression.' We also see huge and growing global financial flows. Between 1990 to 2018, international assets and liabilities rose from 128% to 401% of GDP.

Global economy: Transnational corporations are hugely powerful and influence governments. US companies recently, for instance, inhibited US Government responses to Chinese economic espionage (PBS, 2019). Global supply chains matter. World trade rocketed from 39% of GDP in 1990 to 58% in 2018.

Cyber/information: The idea of the internet as a borderless world where national sovereignty didn't matter was hopelessly naïve. But flows of information across borders are vast and growing, with one estimate that the volume of data crossing borders rose by 64 times over the past decade. Moreover, global 'cyber' deeply penetrates all societies now except the most poor or isolated like North Korea.

Infectious diseases: By definition a pandemic is global (WHO, 2010).

Outer Space is a 'commons.' It is a resource that cannot be owned in whole or part and is accessible to all – just like the commons of 'Olde Englande' where the local community could all herd their sheep (Wright, 2019, v2, *Mindspace*).

Notes: Financial, trade and data figures from (The Economist, 2019). This box draws on Wright, 2019, v2, Global Strategy amidst the globe's cultures, available at www.intelligentbiology.co.uk.

[42] My definition differs from those where the global system simply comprises states like billiard balls. It recognises both that states matter *and* also that much about our interconnected global system is best understood at other scales. Either perspective alone taken to an extreme is deeply impractical as it misses much that matters.

(5) Power from US centrality in global information flows

Summary: *The US benefits mightily from its position astride global information flows, from telecoms to finance. Partly inherited from Britain, immense hard work maintained this strength. For 2031, 6G could threaten the Five Eyes' advantage in telecoms; while digital currencies like Monero, Diem, an "e-euro" or "e-renminbi" threaten US centrality in financial information flows. China now benefits from its centrality in global supply chain information flows. Reinforcing the status quo* ***and*** *adapting fast enough to tech change are both key. At global scale this requires* ***"managed openness"*** *to build innovative responses domestically and via networks—from the closest allies on outwards—that balance security and the benefits of connection.*

Every digital message needs a physical route. An analysis of 2.5 billion modern internet routing paths suggests that just under half the observed traffic travels through at least one more nation than is geographically necessary, often a "Five Eyes" country: the US, Canada, UK, Australia, and New Zealand (Buchanan, 2020, Chapter 1). The Five Eyes control much of the switching station and cable infrastructure that carries internet traffic around the world. The US has "transit authority" for information that passes through its borders. US law binds many major Internet companies headquartered in the US. Put simply, the US occupies a remarkable position in global information flows.

The US gains strategic power from this central position in three ways:

- Surveillance of information to enhance situational awareness E.g. in the global war on terror;
- Taking action via its control of global information "choke points." E.g. in global finance to impose sanctions or limit terrorist finance[43]; and
- Earning dividends from its central position[44], E.g. Facebook's 2,979 million or YouTube's 2,291 million global active users in April 2021 (Kemp, 2021) provide vast integrated datasets on global consumer markets that firms from no other country can match. A company like China's WeChat may be hugely successful with some 1,225 million active users in April 2021, but using largely Chinese population data to get insights on European consumer habits only gets you so far (Beattie, 2019).

By 2031, the US faces the danger of losing these advantages. Initially the US may lose its advantages while no other power gains them. That could occur, for example, if the EU continues to pursue its desire for technological sovereignty[45] and continues to seek to lessen EU vulnerability to US sanctions as it did in the wake of recent battles over Iran policy (Brunsden et al., 2021) – as these EU actions would amplify ongoing Chinese and Russian strategies like the Belt and Road Initiative that seek to

[43] The first two of these ways were also suggested in an excellent paper that also introduced the term "weaponized interdependence" (Farrell & Newman, 2019).
[44] The classic example outside information is the financial benefit accruing to the US due to the dollar's central status in global finance, allowing the US to borrow more cheaply. A French President famously called it the "exorbitant privilege."
[45] In February 2020 the European Commission President, Ursula von der Leyen, described her concept of "tech sovereignty", directed as much at the US as China, with the EU contrasted against Silicon Valley and nowhere else (von der Leyen, 2020).

break US centrality. That US loss may be a plausible stepping stone to China gaining, over time, these strategic advantages.

Maintaining US advantages requires both reinforcing the status quo *and* adapting to new technologies. We next consider three areas, two of current US and one of current Chinese information advantage.

Global financial information flows in 2031 – SWIFT, the dollar and blockchain: The US currently benefits greatly from information flows through a global financial network called "SWIFT", the Society for Worldwide Interbank Financial Telecommunication. It plays a critical role authorizing transactions, authenticating parties, and recording exchanges. SWIFT is a cooperative run by representatives from the financial institutions involved, and it is currently a dominant provider: by 2016 it served some 200 countries, 11,000 financial institutions and carried more than 6.5 billion messages annually (Farrell & Newman, 2019).

After 9/11 SWIFT secretly served as a global surveillance tool for the U.S. against terrorism (Farrell & Newman, 2019). SWIFT is also a tool for action: in 2018 the US reimposed SWIFT restrictions on Iran. But that latter action went against EU wishes and the German Foreign Minister, for example, discussed whether the EU should build alternatives less vulnerable to US pressure (Farrell & Newman, 2019).

By 2031, the EU may have built alternatives to SWIFT that will have amplified Russian and Chinese efforts to circumvent US abilities (The Economist, 2020). A blow. But losing US benefits from SWIFT is far from the deepest potential blow to US power.

Truly underpinning US centrality is the dollar's global role. In 1944 the Allies set up the post-War "Bretton Woods" global economic order that fixed participating currencies to the US dollar, which was in turn pegged to gold. In 1971 that system collapsed when US President Nixon let the dollar float. But with continued US economic and political heft and no plausible alternative anchor, out of that chaos emerged a new global economic order ("Bretton Woods II") also dominated by the dollar (Tooze, 2021).

The US problem is that now the US comprises a smaller part of the world economy. As the then Bank of England governor, Mark Carney, noted at a 2019 meeting of the world's central bankers: the US now comprises only 10 per cent of global trade and 15 per cent of global gross domestic product, but the dollar is used to price half of trade invoices and two-thirds of global securities issuance (Greeley, 2019). Such distortions reduce the dollar's ability to emerge still dominant from disruption.

By 2031, these distortions will likely have grown, particularly if China has become the world's largest economy (Cheng & Lee, 2021) and if the EU has pursued its plans for greater autonomy from the US dollar (Brunsden et al., 2021). In March 2021 euro-zone leaders said that boosting the euro's international use would help them achieve "strategic autonomy" (The Economist, 2021c).

The weaker strategic position of the dollar matters because we are likely to experience a period of technological disruption to which the dollar must successfully adapt: disruption from digital currencies. What challenges do they pose?

- The $1.5 trillion **cryptocurrency** market has grown rapidly since emerging after the global financial crisis, offering a vision of money free from central bank control (Stacey, 2021). Cryptocurrencies are pieces of digital code that are traded as an asset. They are built on blockchain, a decentralized ledger technology that offers a permanent record of transactions divided among different nodes. Bitcoin is the oldest, launched in 2009, and has a market value of around $700bn. US authorities are only beginning to grip this challenge. The US Treasury last month announced cryptocurrency transfers worth $10,000 or more to be reported to the US tax authorities. Such currencies threaten US situational awareness and ability to act. That is compounded by new, potentially untraceable "privacy coins" like "Monero", which is rising in popularity among cybercriminals and ransomware gangs (Murphy, 2021).
- Some cryptocurrencies, called **stablecoins** claim to be pegged to other assets, including traditional "fiat" currencies like the US dollar. However, these lack consumer protections and provide poor accounts of their reserves (Stacey, 2021). The Facebook-backed stablecoin Libra has been renamed Diem, which could launch this year. But they bring enormous potential for financial instability as central banks lose power over monetary policy (Szalay & Venkataramakrishnan, 2021), a non-trivial issue as the global financial crisis showed. Huge privacy issues are raised if a company like Facebook controlled vast amounts of financial data. Moreover, if a stablecoin acquired billions of users across borders (something Facebook already has) that will at a minimum disrupt US capabilities and the dollar's centrality.
- **Central bank digital currencies (CBDCs)** are official efforts to create a digital version of money using distributed ledger technology. CBDCs are central banks' attempts to keep control of the monetary and payments system (Szalay & Venkataramakrishnan, 2021). China is already trialing one, while the UK and EU are considering them. What are the threats? A challenge for democracies—although not authoritarian regimes—is that CBDCs can provide vast data on populations. Creative solutions involving private banks may get around privacy concerns – but however a CBDC is implemented it will cause far-reaching changes to both domestic and cross-border financial mechanisms (Bank for International Settlements, 2021). The rise of digital currencies, as the EU is considering, might result in a new global equilibrium where many currencies share global reserve-currency status – and that could provide space for China's yuan, which has its own global aspirations but is hampered now by its lack of convertibility (The Economist, 2021c). Japan's top financial diplomat warned in October 2020 of China's fast pace developing a CBDC because "First-mover advantage is something we should be afraid of", where China's CBDC will set the standards and the "technology platform which would facilitate further wide adoption" (Wilson, 2020). Chinese authorities are working feverishly prepare for tens of thousands of foreign athletes and fans at the February 2022 Winter Olympics to use its digital currency, "an important political task" as People's Bank of China deputy governor Fan Yifei said

recently (Liu & McMorrow, 2021). If nothing else, a Chinese CBDC deeply embedded within global systems built to Chinese preferences would give China an incredible source of information.

The US in 2021 gains huge benefits from its central position in the global financial system, but this also means the US has by far the most to lose by 2031. To retain its advantage the US must adapt.

How can the US adapt to ride these technological changes in global finance? No strategy can be too prescriptive, and strategy must respond to how digital currencies, systems like SWIFT or payments develop. But some forethought is needed to try and stay in touch with competitors. And whatever strategy is pursued should involve:

- Developing new effective regulation of cryptocurrencies;
- Preventing global corporations like Facebook setting up new stablecoins that weaken the dollar but sit outside US control. The plans for a Swiss-based Libra would have done exactly that. The renamed “Diem” now seems to be moving to the US (Browne, 2021), but even then harnessing Facebook’s near 3 billion active users must disrupt the dollar’s position and at a minimum should be thought through.
- The US must lead on global thinking about CBDCs, which is not currently the case. This does not mean acting rashly in headlong pursuit of novelty; but neither can it mean burying one’s head in the sand. There is a reasonable chance that stablecoins and/or CBDCs in some form will be significant in 2031 – and this requires official, thinktank and academic analysis and options to retain US advantages. For example, it may be that the existing dollar can be repurposed, but that needs to be thought through. "We already have a digital currency in this country, it’s called the dollar," said Richmond Fed Bank President Thomas Barkin on June 28th 2021, and he went on that if the US pursues change then "We ought to have a sense of what are we trying to accomplish when we do it”. That is true, but with an eye to keeping US strategic advantage relative to self-declared competitors like the euro and renminbi in 2031.

The trajectory of competition in global financial information flows is highly uncertain, but major disruption poses significant threats and opportunities that the US should anticipate and shape.

Telecoms and global information flows in 2031: The US inherited control of the global telecommunication system’s backbone from the British after World War Two and have skillfully adapted and rebuilt it ever since (Buchanan, 2020).

US centrality is possible because these global systems are more concentrated than might first appear. Roughly 300 cables carry ninety-seven percent of intercontinental internet traffic (Asia-Pacific Economic Cooperation Secretariat, 2013) The dependence on such cables was illustrated in 2008 when a ship’s anchor severed two cables (FLAG Europe Asia and SEA-ME-WE-4) off the coast of Egypt and shut down much of the internet in the Middle East and South Asia. The cloud is also concentrated: 70 percent of all web traffic from the world, on a daily basis, passes through Amazon Web Services data center in Loudoun County, Virginia (CBS News, 2017).

Routing data through Five Eyes nations, US "transit authority" for information, leverage over US headquartered companies, incredible US cryptographic and supercomputing capabilities – these all combine to enable a Five Eyes approach that can be described as Nobody But Us or "NOBUS" (Buchanan, 2017). That is, set the cryptographic bar high enough to secure one's own information against everything except the Five Eyes' signals intelligence capabilities.

But again incredible US strength from its centrality in telecoms also gives the US most to lose if it fails to adapt, as the UK and then US have so successfully for over a century. Three threats are perhaps most significant for 2031.

- First, **6G threatens the Five Eyes**. Standards for how digital devices communicate will matter ever more towards 2031 as the numbers of devices and their information flows increase – and these provide ample espionage opportunities. The US and its allies failed to dominate 5G that is being rolled out globally now (Box 6). 6G standards are now beginning to be developed and 6G will be likely rolling out in 2031 (Box 6). The US and its allies must do better with 6G, or an ever thicker layer of Chinese-permeated technology will overlay much of the globe's digitizing societies.
- Second, who will connect the **next three billion humans** to the internet? In April 2021 about a billion people in Africa, a billion in South Asia, over 200 million in South East Asia and so on are unconnected to the internet (Kemp, 2021). All sites of geopolitical contest, who will build the infrastructures that connect them?

  Consider Africa, which is being connected now. Chinese companies including Huawei, ZTE and China Telecom are major providers of backbone and last-mile technology in Africa, with an eye on wider rollout of mobile and fixed-line infrastructure (Economist Intelligence Unit, 2021). Huawei has deep roots in Africa that provide a solid, perhaps irreversible, foothold for regional expansion. China will soon lay the final stretch of a cross-border fiber-optic cable in Pakistan that forms the backbone of its Digital Silk Road and will support China's digital expansion across Africa. The cable will connect to the submarine PEACE cable in the Arabian Sea that links to various entry points in Africa, providing countries participating in the Belt and Road Initiative with enhanced access to the Chinese tech sector while reducing reliance on western-developed and controlled cable services.
- Third, **computing advances** may radically disrupt security across the global telecoms infrastructure. China's highly capable AI—remember Wu Dao 2.0 described above?—may reduce the scale of the US advantage in cryptography. Quantum computing may, if it works, radically change the requirements for secure communication. Such disruptions could provide a window of opportunity for a capable competitor to exploit in order to catch up. An analogy is the impact of the launch of the British battleship HMS *Dreadnought* in 1906 that rendered all previous battleships obsolete, thus nullifying Britain's previously overwhelming naval superiority and giving Germany an opportunity to catch up.

The US faces transition risks as the global telecoms are rebuilt, and must seek to anticipate and mitigate those risks.

Global value chains and their convergence in China as the workshop of the world: China is not the first workshop of the world—nineteenth century Britain and the mid-twentieth century US were there before—but China's position is different because new information flows have enabled a new character of globalization since around 1990.

Richard Baldwin's book *The Great Convergence* (Baldwin, 2016) describes how the information and communication technology (ICT) revolution around 1990 allowed G7 firms to separate the stages of production and reduce costs by relocating some stages to developing nations.[46] Think "designed in California" and "assembled in China" that may be inscribed on the device you are reading right now. Knowledge poured across borders into China. Baldwin gives a great sports analogy comparing globalisation before and after 1990 (p. 6):

> *"Imagine two soccer clubs sitting down to discuss an exchange of two players. If a trade actually occurs, both teams will gain. Each gets a player of a type they really needed in exchange for a type of player they need less.*
>
> *Now consider a very different type of exchange. Suppose on the weekends, the coach of the better team starts to train the worse team. The outcome of this will surely make the league more competitive overall and it will surely help the worse team. But it is not at all sure that the best team will win from this exchange—even though their coach will profit handsomely from being able to sell his know-how to two teams instead of one."*

That new globalization put China at the center of global information flows that taught it how to build things to create value. So many global value chains run through China and it has learnt so much about so many fields that any other single country will struggle to compete. Indeed, a June 2021 study by Nikkei Asia showed that China had just ousted Taiwan as Apple's biggest source of suppliers (Ting-Fang & Li, 2021). Even with US political will, moving supply chains out of China is expected to be a slow process, and even then it will likely lead many companies by setting up some production elsewhere (e.g. Vietnam or India) rather than moving everything out of China (Hille, 2020).

Knowledge is power, and China sits at the center of global information flows for manufacturing processes that it can turn into an unrivalled knowledge of manufacturing and global value chains.

Recommendation III.5. Reinforcing the status quo[47] **and** adapting fast enough to

[46] Despite this important insight, Baldwin's book makes an almost inexplicable error when seeking to explain why a new character of globalisation emerged around 1990 – he fails to acknowledge that around 1990 not only did ICT change but also the Cold War ended, and the end of the Cold War almost certainly contributed to this new character of globalisation. His example of extensive German links to Poland, for instance, clearly relate in part to regime change in Poland.

[47] Scholar Wyatt Hoffman (private correspondence) raises an important question about this recommendation (presaged on pp. 46-7 above): is the US *able* to hold onto the big advantages from network effects it currently enjoys? If not, this suggests a more modest but attainable goal could be to prevent China from gaining those advantages. He notes a distinction between developments that diffuse

tech change are both key. At global scale this requires **"managed openness"** to build innovative responses domestically and via networks—from the closest allies on outwards—that balance security and the benefits of connection.

Conclusion

The character of information in strategy will be different in 2031. Failure to anticipate and respond effectively to this new character could be as catastrophic for the United States—in 2031—as it was for the allied armies who faced the *Panzer* forces and *Blitzkrieg* in May 1940. And at least in July to October 1940 the Royal Air Force's Fighter Command could harness information just as decisively for defense, to win the Battle of Britain. The world's first integrated air defense system challenged ideas that had dominated inter-war thinking on air power—"the bomber will always get through"—and shot them down in flames.

Neither the German hammer nor the British shield were built in 1940. Years before, both had been forged by those like Germany's Heinz Guderian (a principal architect of *Panzer* forces) or Britain's Hugh Dowding (the pioneering leader of Fighter Command), who looked ahead to exploit the future character of information in human conflict.

In 2031, who will have the modern analogues of *Panzer* forces or Fighter Command? Who will have the equivalent of the signals intelligence advantages Britain gained by decrypting Germany's enigma machines? Who will have the vast reserves of manufacturing strength and knowledge that took the US from producing 5,856 aircraft in 1939 to 85,898 by 1943 (Kennedy, 1988, p. 455)? Who will have superiority in data, in information, in knowledge, and in the wiser decision-making that can integrate across the multiple instruments of national power?

The United States is better placed than any other country—including China—to respond effectively and shape the character of information in strategy over the next decade. But only if it thinks ahead.

power (e.g. cryptocurrencies) and those potentially concentrating power (e.g. 5/6G leadership). Instead of attempts to prevent diffusion of US power, which may damage cooperation with allies and partners like Germany, it may be more feasible to focus on preventing Chinese moves to concentrate power in its hands (e.g. gaining 6G leadership). Such an alternative goal is consistent with the main points above – the key is to anticipate these challenges and develop strategies that can begin to meet them.

References

Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis*, *16*(1), 3–9.

Acton, J. M. (2018). Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security*, *43*(1), 56–99. https://doi.org/10.1162/isec_a_00320

Future Defense Spending: Nuclear Modernization, (2021) (testimony of James M. Acton). https://carnegieendowment.org/2021/03/23/future-defense-spending-nuclear-modernization-pub-84147

Andrew, C. (2004). Intelligence, International Relations and "Under-theorisation." *Intelligence and National Security*, *19*(2), 170–184. https://doi.org/10.1080/0268452042000302949

Arnold, M., & Romei, V. (2021, April 13). Eurozone's economy shows signs of adapting to lockdowns. *Financial Times*. https://www.ft.com/content/b756bab9-43a7-49c6-a3de-c98e891a0aea

Asia-Pacific Economic Cooperation Secretariat. (2013). *Economic Impact of Submarine Cable Disruptions*. https://www.apec.org/Publications/2013/02/Economic-Impact-of-Submarine-Cable-Disruptions

Baldwin, R. (2016). *The Great Convergence: Information Technology and the New Globalization* (First Edition edition). Harvard University Press.

Bank for International Settlements. (2021). *III. CBDCs: An opportunity for the monetary system*. https://www.bis.org/publ/arpdf/ar2021e3.htm

Beattie, A. (2019, July 24). Technology: How the US, EU and China compete to set industry standards. *Financial Times*. https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Browne, R. (2021, May 12). *Facebook-backed crypto project Diem abandons Swiss license application, will move to the U.S.* CNBC. https://www.cnbc.com/2021/05/12/facebook-backed-diem-is-moving-from-switzerland-to-the-us.html

Brunsden, J., Fleming, S., & Stafford, P. (2021, January 16). EU sets out plans to curb reliance on dollar in post-Trump era. *Financial Times*. https://www.ft.com/content/20f39e33-e360-479e-82e2-5441d24f0e0b

Buchanan, B. (2017). *Nobody but us: The rise and fall of the golden age of signals intelligence*. Hoover Institution.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (1st edition). Harvard University Press.

Cater, L. (2021, June 3). *The EU has introduced a new 'digital' ID. Here's what it means for you.* POLITICO. https://www.politico.eu/article/eu-europe-digital-id/

CBS News. (2017). *The heart of "The Cloud" is in Virginia*. https://www.cbsnews.com/news/cloud-computing-loudoun-county-virginia/

Chen, J., Walz, E., Lafferty, B., McReynolds, J., Green, K., Ray, J., & Mulvenon, J. (2018). *China's Internet of Things | Report for the U.S.- China Economic and Security Review Commission*. SOSi. https://www.uscc.gov/research/chinas-internet-things

Cheng, E., & Lee, Y. N. (2021, February 1). *New chart shows China could overtake the U.S. as the world's largest economy earlier than expected*. CNBC. https://www.cnbc.com/2021/02/01/new-chart-shows-china-gdp-could-overtake-us-sooner-as-covid-took-its-toll.html

Churchill, W. S. (1948). *The Gathering Storm*. Cassell & Co Ltd.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press.

Clausewitz, C. von. (2008). *On War* (M. Howard & P. Paret, Trans.). Oxford University Press.

Cyberspace Solarium Commission. (2020). *Cyberspace Solarium Commission Report*. Cyberspace Solarium Commission. https://www.solarium.gov/report

Defense Science and Technology Laboratory. (2020). *Joint Emerging Technology Trends*. Her Majesty's Government.

Department of Defense. (2018). *Joint Concept for Operating in the Information Environment*. United States Department of Defense.

Dougherty, C. (2014, September 5). *The Most Terrifying Lesson of World War I: War Is Not Always "Short and Sharp"* [Text]. The National Interest; The Center for the National Interest. https://nationalinterest.org/feature/the-most-terrifying-lesson-world-war-i-war-not-always-short-11207

Economist. (2021a, January 23). Chipmaking is being redesigned. Effects will be far-reaching. *The Economist*. https://www.economist.com/business/2021/01/23/chipmaking-is-being-redesigned-effects-will-be-far-reaching

Economist. (2021b, January 23). *The struggle over chips enters a new phase*. https://www.economist.com/leaders/2021/01/23/the-struggle-over-chips-enters-a-new-phase

Economist Intelligence Unit. (2021). *Africa-China relations—Taming the dragon: New frontiers of co-operation?* https://www.eiu.com/public/topical_report.aspx?campaignid=mar21africachinaWP

European Commission. (n.d.). *European Digital Identity* [Text]. European Commission - European Commission. Retrieved June 22, 2021, from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
Exeter University. (n.d.). *Digital Object Architecture and IoT standardisation*. Retrieved February 18, 2020, from http://www.internetpolicystreams.com/news/item/362-digital-object-architecture-and-iot-standardisation
Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351
Fildes, N. (2021, June 14). Vodafone hands first 'open RAN' deals to Samsung, Dell and NEC. *Financial Times*. https://www.ft.com/content/338ad9aa-0a4b-4f7c-bcc4-beddb994f884
Floridi, L. (2010). *Information: A Very Short Introduction* (Illustrated edition). OUP Oxford.
Freedman, L. (2013). *Strategy: A History*. OUP USA.
Friston, K. (2010). The free-energy principle: A unified brain theory? *Nature Reviews Neuroscience*, *11*(2), 127–138.
Future Today Institute. (2021). *2021 Tech Trends Report*. Future Today Institute.
Giles, K., & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. *Cyber Conflict (CyCon), 2013 5th International Conference On*, 1–17. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6568390
Goldfarb, A., & Lindsay, J. (2020). *Artificial intelligence in war: Human judgment as an organizational strength and a strategic liability*. Brookings Institution. https://www.brookings.edu/research/artificial-intelligence-in-war-human-judgment-as-an-organizational-strength-and-a-strategic-liability/
Gorman, L. (2020). *A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything*. The German Marshall Fund of the United States. https://securingdemocracy.gmfus.org/future-internet/
Gray, C. S. (2010). War-continuity in change, and change in continuity. *Parameters*, *40*(2), 5.
Greeley, B. (2019, August 25). Central bankers rethink everything at Jackson Hole. *Financial Times*. https://www.ft.com/content/360028ba-c702-11e9-af46-b09e8bfe60c0
Grossmann, I. (2017). Wisdom in Context. *Perspectives on Psychological Science*, *12*(2), 233–257. https://doi.org/10.1177/1745691616672066
Gruber, J., & Johnson, S. (2019). *Jump-Starting America: How Breakthrough Science Can Revive Economic Growth and the American Dream*. Hachette UK.
Handel, M. I. (1981). *The diplomacy of surprise, Hitler, Nixon, Sadat*. Center for International Affairs, Harvard University.
Harrison, T., Johnson, K., Moye, J., & Young, M. (2021). *Space Threat Assessment 2021*. Center for Strategic and International Studies. https://www.csis.org/analysis/space-threat-assessment-2021
Heikkilä, M. (2021, June 9). *Meet Wu Dao 2.0, the Chinese AI model making the West sweat*. POLITICO. https://www.politico.eu/article/meet-wu-dao-2-0-the-chinese-ai-model-making-the-west-sweat/
Hille, K. (2020, October 6). The great uncoupling: One supply chain for China, one for everywhere else. *Financial Times*. https://www.ft.com/content/40ebd786-a576-4dc2-ad38-b97f796b72a0
Hitchens, T. (2020, June 18). Shifting Gears, DoD Moves To LEO For Future OPIR Sats. *Breaking Defense*. https://breakingdefense.com/2020/06/shifting-gears-dod-moves-to-leo-for-future-opir-sats/
HM Treasury. (2018). *The Green Book: Central Government guidance on appraisal and evaluation*.
Hoffman, W. (2021). *AI and the Future of Cyber Competition*. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/ai-and-the-future-of-cyber-competition/
Home Office. (2019). *Future technology trends in security*. Her Majesty's Government. https://www.gov.uk/government/publications/future-technology-trends-in-security
Howard, M. (1976). *War in European History*. Oxford University Press. https://books.google.co.uk/books/about/War_in_European_History.html?id=Bi_cAAAAMAAJ&redir_esc=y
Ichikawa, J. J., & Steup, M. (2018). The Analysis of Knowledge. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Summer 2018). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2018/entries/knowledge-analysis/
ICO. (2017). *Big data, artificial intelligence, machine learning and data protection v. 2.2*. Information Commissioner's Office. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
IPlytics. (2021, February 16). Who is leading the 5G patent race? *IPlytics*. https://www.iplytics.com/report/5g-patent-race-02-2021/
Jackson, K., Kidder, K. L., Mann, S., Waggy, W. H., Lander, N., & Zimmerman, S. R. (2020). *Raising the Flag: Implications of U.S. Military Approaches to General and Flag Officer Development*. https://www.rand.org/pubs/research_reports/RR4347.html
Johnson, D. D., & Tierney, D. (2011). The Rubicon theory of war: How the path to conflict reaches the point of no return. *International Security*, *36*(1), 7–40.

Kazmierczak, M., Ritterson, R., Gardner, D., Casagrande, R., Hanemann, T., & Rosen, D. H. (2019). *China's Biotechnology Development: The Role of US and Other Foreign Engagement: a Report Prepared for the US-China Economic and Security Review Commission*. Gryphon Scientific.
Keegan, J. (1993). *A History of Warfare*. Pimlico.
Kemp, S. (2021, April 22). WhatsApp is the World's Favorite Social Platform (And Other Facts). *Social Media Marketing & Management Dashboard*. https://blog.hootsuite.com/simon-kemp-social-media/
Kennedy, P. (1988). *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500-2000*. Unwin Hyman.
Kilcullen, D. (2013). *Out of the Mountains: The Coming Age of the Urban Guerrilla*. Oxford University Press.
Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 1097–1105.
Lazanki, D. (n.d.). *The Problem With the United Nations Setting Tech Standards for Your Internet Devices*. Council on Foreign Relations. Retrieved February 17, 2020, from https://www.cfr.org/blog/problem-united-nations-setting-tech-standards-your-internet-devices
Lee, K.-F. (2018). *AI Superpowers: China, Silicon Valley, and the New World Order*. Houghton Mifflin Harcourt.
Lewis, J. A. (2010). *Thresholds for Cyberwar*. https://www.csis.org/analysis/thresholds-cyberwar
Libicki, M. (2019). A Hacker Way of Warfare. In N. D. Wright (Ed.), *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press.
Liu, N., & McMorrow, R. (2021, August 2). China's digital renminbi will go for gold at Beijing Games. *Financial Times*. https://www.ft.com/content/0cc6720b-2089-41e2-9204-7599b48a82af
Martin, D. A., Shapiro, J. N., & Ilhardt, J. G. (2020). *Trends in Online Influence Efforts (V.2.0)*. https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf
McInnis, K. J., & Rollins, J. W. (2021). *The National Security Council: Backgroundand Issues for Congress*. Congressional Research Service.
Morgan, F. E., Mueller, K. P., Medeiros, E. S., Pollpeter, K. L., & Cliff, R. (2008). *Dangerous Thresholds*. Rand.
Morgan, P. M. (1985). Saving face for the sake of deterrence. In R. Jervis, R. N. Lebow, & J. G. Stein (Eds.), *Psychology and Deterrence*. JHU Press.
Murgia, M., Yang, Y., & Gross, A. (2019, December 1). *Chinese tech groups shaping UN facial recognition standards*. Financial Times. https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67
Murphy, H. (2021, June 22). Monero emerges as crypto of choice for cybercriminals. *Financial Times*. https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6
Nakasone, P. M., & Sulmeyer, M. (2021, March 17). *How to Compete in Cyberspace*. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity
NATO Science & Technology Organization. (2020). *Science & Technology Trends 2020-2040*. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf
Nikkei Asia. (2021, April 18). *US and Japan to invest $4.5bn in next-gen 6G race with China*. Nikkei Asia. https://asia.nikkei.com/Business/Telecommunication/US-and-Japan-to-invest-4.5bn-in-next-gen-6G-race-with-China
Office of Communications. (2021). *Technology Futures: Spotlight on the technologies shaping communications for the future*. Her Majesty's Government. https://www.ofcom.org.uk/__data/assets/pdf_file/0011/211115/report-emerging-technologies.pdf
Office of the Director of National Intelligence. (2021). *Global Trends 2040*. https://www.dni.gov/index.php/global-trends-home
Paul, C., Yeats, J. M., Clarke, C. P., Matthews, M., & Skrabala, L. (2015). *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners*. Rand Corporation.
PBS. (2019). *Trump's Trade War*. FRONTLINE. https://www.pbs.org/wgbh/frontline/film/trumps-trade-war/
Peel, M., & Fedor, L. (2021, June 15). Nato warns China's military ambitions threaten global order. *Financial Times*. https://www.ft.com/content/f454033a-9975-4efd-92eb-9cf63306af7f
Peng, G., & Yao, Y. (2005). *The science of military strategy*. Military Science Publishing House.
Perera, D. (2015). *Lawsuit seeks relief from cyberspying - CIA and OPM: Rethinking the silo*. POLITICO. https://www.politico.com/tipsheets/morning-cybersecurity/2015/07/lawsuit-seeks-relief-from-cyberspying-cia-and-opm-rethinking-the-silo-212543
Ponting, C. P. (2017). Big knowledge from big data in functional genomics. *Emerging Topics in Life Sciences*, *1*(3), 245–248. https://doi.org/10.1042/ETLS20170129
Porche, I., Paul, C., York, M., Serena, C. C., & Sollinger, J. M. (2013). *Redefining Information Warfare Boundaries for an Army in a Wireless World*. Rand Corporation.

Propp, K. (2019, December 11). Waving the flag of digital sovereignty. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/
Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare* (Illustrated edition). Macmillan USA.
Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018). *Modern Political Warfare: Current Practices and Possible Responses*. https://www.rand.org/pubs/research_reports/RR1772.html
Romei, V., & Burn-Murdoch, J. (2020, March 22). Real-time data show virus hit to global economic activity. *Financial Times*. https://www.ft.com/content/d184fa0a-6904-11ea-800d-da70cff6e4d3
Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*, *33*(2), 163–180. https://doi.org/10.1177/0165551506070706
Ryan, S. (2020). Wisdom. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2020). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2020/entries/wisdom/
Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Penguin Random House USA.
Schelling, T. C. (1966). *Arms and influence*. Yale University Press.
Schmidt, E., Work, B., Catz, S., Chien, S., Darby, C., Ford, K., Griffiths, J.-M., Horvitz, E., Jassy, A., & Mark, W. (2021). *National Security Commission on Artificial Intelligence (AI)*. National Security Commission on Artificial Intellegence.
Sehl, K. (2021, May 5). 23 Important TikTok Stats Marketers Need to Know in 2021. *Social Media Marketing & Management Dashboard*. https://blog.hootsuite.com/tiktok-stats/
Sharot, T., Korn, C. W., & Dolan, R. J. (2011). How unrealistic optimism is maintained in the face of reality. *Nature Neuroscience*, *14*(11), 1475–1479.
Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.
Smeets, M. (2019, May 28). Cyber Command's Strategy Risks Friction With Allies. *Lawfare*. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies
Spain, E. (2020, November 1). Reinventing the Leader Selection Process. *Harvard Business Review*. https://hbr.org/2020/11/reinventing-the-leader-selection-process
Stacey, K. (2021, June 9). US financial regulator warns against strict cryptocurrency rules. *Financial Times*. https://www.ft.com/content/ae0d40a1-8a4a-4885-a6a7-b157e27b3311
Straus, S. G., Krueger, T. C., Grimm, G. E., & Giglio, K. (2018). *Malleability and Measurement of Army Leader Attributes: Personnel Development in the U.S. Army*. https://www.rand.org/pubs/research_reports/RR1583.html
Szalay, E., & Venkataramakrishnan, S. (2021, May 28). What are cryptocurrencies and stablecoins and how do they work? *Financial Times*. https://www.ft.com/content/424b29c4-07bf-4612-b7d6-76aecf8e1528
Tertrais, B. (2011). Extended deterrence: Alive and changing. *The Interpreter–Lowy Institute for International Policy*.
The Economist. (2019, January 24). Globalisation has faltered. *The Economist*. https://www.economist.com/briefing/2019/01/24/globalisation-has-faltered
The Economist. (2020, May 7). The financial world's nervous system is being rewired. *The Economist*. https://www.economist.com/special-report/2020/05/07/the-financial-worlds-nervous-system-is-being-rewired
The Economist. (2021a, May 15). *SpaceX, a Tesla for the skies | The Economist*. https://www.economist.com/business/2021/05/13/spacex-a-tesla-for-the-skies
The Economist. (2021b, June 5). The new geopolitics of global business. *The Economist*. https://www.economist.com/leaders/2021/06/05/the-new-geopolitics-of-global-business
The Economist. (2021c, June 24). The international role of the euro. *The Economist*. https://www.economist.com/finance-and-economics/2021/06/24/the-international-role-of-the-euro?frsc=dg%7Ce
Ting-Fang, C., & Li, L. (2021, June 6). China ousts Taiwan as Apple's biggest source of suppliers. *Financial Times*. https://www.ft.com/content/d2c9be25-6da2-47d4-9756-793a13738cf4
Tooze, A. (2021, January 15). The Rise and Fall and Rise (and Fall) of the U.S. Financial Empire. *Foreign Policy*. https://foreignpolicy.com/2021/01/15/rise-fall-united-states-financial-empire-dollar-global-currency/
Volz, D., & McMillan, R. (2021, March 10). Massive Hacks Linked to Russia, China Exploited U.S. Internet Security Gap. *Wall Street Journal*. https://www.wsj.com/articles/massive-hacks-linked-to-russia-china-exploited-u-s-internet-security-gap-11615380912
von der Leyen, U. (2020, February 19). *Op-ed by Commission President von der Leyen* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260
Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Walker, C., & Ludwig, J. (2021). *Sharp Power and Democratic Resilience Series | A Full-Spectrum Response to Sharp Power*. National Endowment for Democracy. https://www.ned.org/sharp-power-and-democratic-resilience-series-a-full-spectrum-response-to-sharp-power/
Walt, S. M. (2020). The United States Forgot Its Strategy for Winning Cold Wars. *Foreign Policy*. https://foreignpolicy.com/2020/05/05/offshore-balancing-cold-war-china-us-grand-strategy/
Weinberger, D. (2010). The problem with the data-information-knowledge-wisdom hierarchy. *Harvard Business Review*, *2*.
WHO. (2010). *WHO | What is a pandemic?* WHO. https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/
Wilson, T. (2020, October 8). China seeking first-mover advantage in building digital currency: Senior Japan official. *Reuters*. https://www.reuters.com/article/us-cenbanks-digital-idUSKBN26T2MF
Wolpert, L. (2010). *How We Live and Why We Die: The secret lives of cells*.
World Bank. (2021). *World Development Report 2021: Data for Better Lives*. The World Bank.
Wright, N. D. (2014). Neural prediction error is central to diplomatic and military signalling DiEuliis D, Casebeer W, Giordano J, Wright ND, Cabayan H (Eds). In D. DiEuliis, W. Casebeer, J. Giordano, N. D. Wright, & H. Cabayan (Eds.), *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World*. US DoD Joint Staff.
Wright, N. D. (2017). *From control to influence: Cognition in the Grey Zone* (p. 159). University of Birmingham, UK. www.nicholasdwright.com/publications
Wright, N. D. (2018). *Getting Messages Through: The cognition of influence with North Korea and East Asia*. Intelligent Biology.
Wright, N. D. (2019a). *From control to influence: Cognition in the Grey Zone (v3)* (p. 158). Intelligent Biology. www.intelligentbiology.co.uk
Wright, N. D. (Ed.). (2019b). *Artificial Intelligence, China, Russia, and the Global Order*. Air University Press.
Wright, N. D. (2019c). *Global Strategy amidst the globe's cultures: Cultures in individual cognition, states and the global system (v2)*. Intelligent Biology. www.intelligentbiology.co.uk
Wright, N. D. (2020). *Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challenge*. National Endowment for Democracy. https://www.ned.org/sharp-power-and-democratic-resilience-series-artificial-intelligence-and-democratic-norms/
Wright, N. D., Giordano, J., & DiEuliis, D. (2021, February 21). *3 Tricks for Strategically Competing in the Global Innovation Smackdown*. The National Interest; The Center for the National Interest. https://nationalinterest.org/feature/3-tricks-strategically-competing-global-innovation-smackdown-178456
Wright, N. D., Rees, G., & Lewis, J. A. (2021, May 26). *Innovation with Allies: Practical Paths Forward* [Center for Strategic and International Studies]. https://www.csis.org/analysis/innovation-allies-practical-paths-forward
Wright, N. D., & Sadjadpour, K. (2014, January 14). The Neuroscience Guide to Negotiations With Iran. *The Atlantic*.
Zenko, M. (2015). *Red Team: How to Succeed By Thinking Like the Enemy*. Basic Books.
Zhao, S., Moritz, S., & Seal, T. (2021, February 8). Forget 5G, the U.S. and China Are Already Fighting for 6G Dominance. *Bloomberg.Com*. https://www.bloomberg.com/news/features/2021-02-08/forget-5g-the-u-s-and-china-are-already-fighting-for-6g-dominance