Future Dynamics of Warfare

Everyone is a Player
Everything is a Target
Conflict as a Sandbox

Team: Sullivan's Travels

Future Dynamics of Warfare: Everyone is a Player, Everything is a Target Conflict as a Sandbox

By

LTC Joseph "Joe" Bell (USA, Aviation)
COL John Cooper (USA, Human Resources)
LTC Kristine "Kris" Hinds (USAR, Logistics)
LtCol Erik Keim (USMC, Communications)
LTC Michael "Neal" Miller (USAR, Logistics)

Faculty Advisor: Dr. Kathleen Moore

United States War College Class of 2024

About This Document

Team Sullivan's Travels completed this report to meet the Master of Strategic Studies degree requirement from the United States Army War College, Carlisle Barracks, Pennsylvania. This report is based on open-source information and answers a strategic question by Mr. Ian Sullivan, Deputy Chief of Staff, G-2, United States Army Training and Doctrine Command.

Requirement

How will innovations from contemporary conflicts likely shape the future dynamics of warfare, and what does it mean for Large Scale Combat Operations (LSCO) and pacing threats by 2035?

The team produced their findings in multiple mediums, including a digital PDF version and a soft-bound book format. The team used multiple methodologies to determine key findings, which included reviewing scholarly publications, reporting from open sources, and applying the nominal group technique.

Analytic Confidence

Unless otherwise indicated, this analysis has a MODERATE level of confidence. The authors carefully evaluated sources using established tools (Trust Scale and Web Site Evaluation Worksheet); however, additional limitations influenced uncertainty. The question was complex, and the research timeline was relatively short due to the competing USAWC degree requirements. The research team worked individually and collaboratively to answer the questions and utilized several structured analytic techniques. To mitigate some of the identified limitations, advanced artificial intelligence platforms, like Perplexity, Microsoft CoPilot, and Google Gemini, aided in open-source content research and editorial support.

Table of Contents

Key Findings ..... A
Battlefield Visibility: Disruptions by Drone Swarm Advancements 1
Battlefield Visibility: Networked Acoustic Sensors for Integrated Air Defense 3
Battlefield Visibility: Blending in the Electromagnetic Spectrum 5
Battlefield Visibility: Space-to-Cellphone Revolutionizing Military Communications 7
Battlefield Visibility: Virtual Deception Drives Shift in Intelligence-Sharing 9
Rapid Warfare: Lethal Autonomous Weapons Use Certain 11
Rapid Warfare: Rapid War-Time Innovations Required to Compete 14
Rapid Warfare: Free Space Optics and Reliable, Secure Communication 16
Rapid Warfare: Alliances Battle Networks Boosted Through Machine Learning 18
Rapid Warfare: Autonomous Semi-Submersibles for Logistics Resupply 20
Rapid Warfare: Ethical and Legal Dilemmas in Lethal Autonomous Weapon Systems 22
Rapid Warfare: Mind of the Machine: North Korea's Growing AI Threat 25
Rapid Warfare: Contested Logistics Will Benefit from Quantum Computing 27
Lower Barriers: Private Sector Involvement in Future Conflicts 30
Vulnerable Homelands: Cyber Attacks on Critical Infrastructure 33
Vulnerable Homeland: Preparation of the US Defense Industrial Base 36
Vulnerable Homeland: Weaponized Water in Contemporary Conflict 38
Vulnerable Homeland: Fortress Fleet Tactic Usage Highly Likely 41
Vulnerable Homeland: The Money Machine: North Korea's State-Sponsored Hacking 43
Vulnerable Homelands: Foreign Investment in Land and Infrastructure 46
Vulnerable Homelands: Cyber Defenses and Policies Unlikely to Secure Vulnerabilities 48
Other: Alliances Benefit from Multilateral Exercises vs Bilateral 50
Other: Drivers of North Korea's Growing Missile Threat 52
Other: Efforts to Curb North Korea's Nuclear Program Fueled Its Development 54
Other: Foreign Support Won't Fuel North Korea's Nuclear Ambitions 56
Annex A – Terms of Reference i
Annex B – Trust Scale and Web Site Evaluation Worksheet iii
Annex C – Kesselman List of Estimative Words xxiii
Annex D – Innovation Multi-Criteria Decision Analysis xxiv
Annex E – Presentation Slides xxv

Key Findings

How will innovations from contemporary conflicts likely shape the future dynamics of warfare, and what does it mean for Large Scale Combat Operations (LSCO) and pacing threats by 2035?

- What are likely potential changes to future warfighting functions?
- What are the likely impacts on future regional alliances, partnerships, and relationships?

Summarized Conclusion

It is **highly likely (71-86%)** that innovations from recent conflicts will more fully integrate diverse actors into future conflict due to increased entry points enabled by Unprecedented Visibility, Rapid Technology Implementation, Lower Barriers to Entry, and Vulnerable Homelands.

Despite the traditional role of militaries during the conflict, the ubiquity of technology and the treatment of conflict as a testing bed (sandbox) increases the rapid implementation of material and non-material applications by any party.

Unprecedented Visibility

Advancements in intelligence, surveillance, and reconnaissance (ISR), including inexpensive and rapid equipment production and accessibility of space and communications, are highly likely (71-85%) to create an environment of unprecedented visibility, making operations increasingly challenging.

Primary innovations influencing this outcome:

- **Adaptive Integration (Blending, not Hiding).** Hiding is the static act of concealing one's presence. Blending is a proactive and dynamic process that involves assimilating into the environment to take advantage of its inherent patterns, behaviors, and characteristics. This requires altering visual, digital, or electromagnetic signatures.
- **Hybrid Warfare.** The cost-effectiveness, anonymity, reach, and capacity to directly engage with a target population through digital platforms in a connected world increases the number of actors actively engaging in disinformation and propaganda campaigns, manipulating social media, radicalizing individuals online, and directly recruiting and mobilizing for grey zone conflicts.

In Ukraine, local companies produce approximately three thousand drones daily for deployment against Russian forces. The $27 billion global commercial drone market sustains this effort, ensuring a near-constant supply for both sides of any future conflict. To counter this, both countries resorted to countermeasures, including anti-air missiles, Counter Rocket, Artillery, and Mortar (C-RAM) systems, networked acoustic sensors, and a variety of electronic warfare suites.

Over the last decade, companies like SpaceX revolutionized space accessibility through the rapid increase in space launches. This resulted in decreased costs of launching payloads into space and a surge in commercial satellite launches, increasing civilian access to satellite imagery and the ability to task satellites, giving anyone an unprecedented ability to influence conflict.

In communications, one can easily detect, locate, jam, and intercept military-specific radio transmissions. Ukrainians adopted digital camouflage to counter this, blending their transmissions with civilian communications. They exploited Russian vulnerabilities using agile software-defined radio systems for their Electronic Warfare efforts. The Marine Corps is testing a method that involves shifting transmissions from easily detected radio frequencies to nearly undetectable laser beams, increasing the digital bandwidth for further technological advances.

Figure 1 Image shows the comparison of signal dispersion between laser and microwave. Effect Photonics

The role of civilians in the intelligence apparatus grew significantly, with nearly everyone carrying a device capable of capturing and transmitting images or video. Oryx's reporting of Russian equipment highlights the potential of crowdsourcing in the future.

Rapid, Technology Enhanced Warfare

It is highly likely (71-85%) that the rapid implementation and enhanced technological capabilities may increase the employment of information warfare, precision targeting, and tactical maneuver execution.

Primary innovations influencing this outcome:

- **Artificial Intelligence**: Generative and predictive artificial intelligence accelerate and guide tactical and operational decision-making. This increases visibility and targetability across all domains for various actors.
- **Autonomous Systems**: Human-in-the-loop, human-on-the-loop, and human-out-of-the-loop systems enhance the coordination and effectiveness of multi-domains, capabilities, and access points for all participants. The availability of autonomous systems provides a low-cost entry into conflict.

AI allows for rapid employment of information warfare by increasing the speed and potential influence sphere for information. At the onset of the Russian invasion of Ukraine, Russia used AI-guided technology to implore Ukrainians to surrender via a deep-fake video of President Zelensky. This demonstrates an AI-enabled tactic that can influence narratives rapidly.

Israel uses two AI systems, Lavender and Gospel, for precision targeting. Together, these systems enabled Israel to go from identifying 50 targets annually to over 100 daily, thus shortening kill chains. In the Ukraine-Russia war, both sides deployed millions of unmanned aerial vehicles (UAVs) equipped with AI-powered capabilities for surveillance, reconnaissance, and direct attacks. These drones can autonomously navigate complex environments, identify targets, and assess damage after attacks. The demand for these capabilities is only growing. Drones have many applications in military operations and commercial uses. In the military, they are employed for ISR and targeted strikes. Their prevalence in the commercial sector provides increased availability of commercial off-the-shelf items and increased research and development on this technology.

Figure 2 Image depicting the use of Lander and Gospel for AI Generated Kill List. Democracy Now!

Lower Barriers to Entry and Blurred Lines of Conflict

Private sector, non-state actors, and individual citizens are highly likely (71-85%) to play pivotal roles in conflict and pre-conflict dynamics by leveraging commercially available

technologies to conduct operations, gather intelligence, and influence public opinion. This allows broader conflict participation and agenda-driven actors to develop innovative technologies rapidly.

Primary innovations influencing this outcome:

- **Fifth Generation Warfare**: This loosely defined term describes contemporary conflicts in which tactics like social media influence operations and cyberattacks play a more prominent role in warfare.
- **Sixth Domain (Private Sector Involvement)**: Described by the Atlantic Council as the "sphere of activities" of the private sector in warfare. Private sector expertise, reach, and economic strength enable them to participate through cybersecurity, information, logistics, technology, infrastructure, and financial warfare.

Access to affordable technology, connectivity, and anonymity allows average citizens to indirectly participate in cyberattacks, crowdsource information, analyze data from battlefield environments, share intelligence, engage in disinformation campaigns, and disseminate or encounter state-sponsored propaganda. With the rise of "digital dopamine," discussed by Dr. Anna Lembke, author of Dopamine Nation, digital media increases the accessibility to receive and influence content. This, coupled with the rise of digital nodes, allows hackers to conduct offensive cyber-attacks or influence a narrative. At the corporate level, companies like Twitter, Facebook, and Google can police content or steer search results to portray a narrative deemed acceptable by that company.

In Ukraine, the private sector actively leverages cyber, space, and AI to support its chosen side. American tech companies Palo Alto and Microsoft contributed to safeguarding data and protecting Ukrainian networks by setting up firewalls, protecting critical infrastructure, and safeguarding Ukrainian data by migrating the data to foreign servers. Companies offered help based on their own interests, not due to government mandates, and this influenced the course of the war between Ukraine and Russia.

Figure 3 Image depicting the role of private sector in conflict. Morocco World News

Challenges can arise as companies provide "goodwill" support since they wield the power to turn that support off as they deem fit. SpaceX, for example, provided Starlink to the Ukrainians but later denied the service, preventing a Ukrainian drone from attacking a Russian naval fleet.

Vulnerable Homelands

Kinetic and non-kinetic attacks are highly likely (71-85%) to disrupt critical infrastructure and destabilize security in a homeland environment during a future conflict. Vulnerable homelands complicate the security paradigm due to the increased accessibility of targets, the information sphere, and the ability for anyone to impact them.

Primary innovation influencing this outcome:

- **Water Warfare**: Emerging concerns over scarcity in new regions, expanded economic utilization of water, and innovations in artificial intelligence, Internet of Things (IoT), and autonomous systems broadened the capabilities and access to impact water systems.

Essential services depend on Information and Communication Technology (ICT), which enables networked programs and processes through the IoT. The rapid growth of IoT increased the number of entry points for adversaries to find and exploit vulnerabilities. Physical objects now have digital sensors, making everything a potential cyber target. These vulnerabilities transform civilian spaces into conflict zones, where the distinction between combatants and non-combatants blurs.

Cyberattacks have led to obstruction of access to telecommunications and internet services, limited access to money, interrupted access to news, and disruption or denial of access to electricity, heating, and water. A hacker in Oldsmar, FL, targeted the water supply and remotely altered the amount of sodium hydroxide in the water. Employees detected and thwarted a potentially deadly attack.

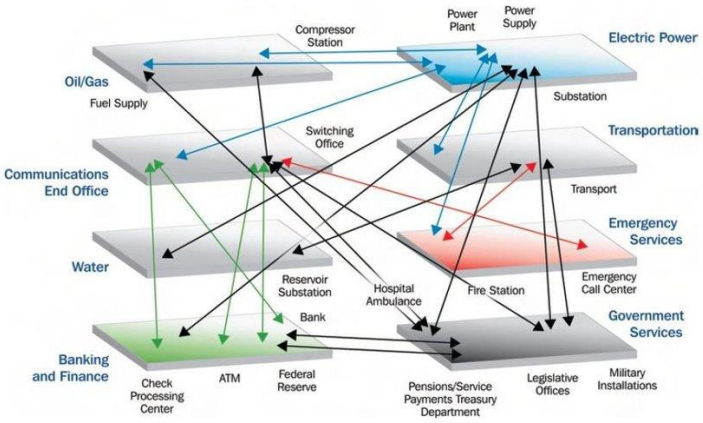


Figure 4 Critical Infrastructure Interdependencies. [Research Gate]

The use of conventional weapons in combination with these cyber operations amplifies the risks to the civilian population. Russia has focused on inflicting damage to the civilian population through a combination of cyber and kinetic attacks – for example, by targeting energy infrastructure during winter. The hacking of Ukraine's largest private energy company, DTEK demonstrates the deliberate targeting of critical civilian infrastructure essential to populations.

The increased access within the information sphere creates a more vulnerable homeland. The spread of disinformation and propaganda undermines trust in institutions through

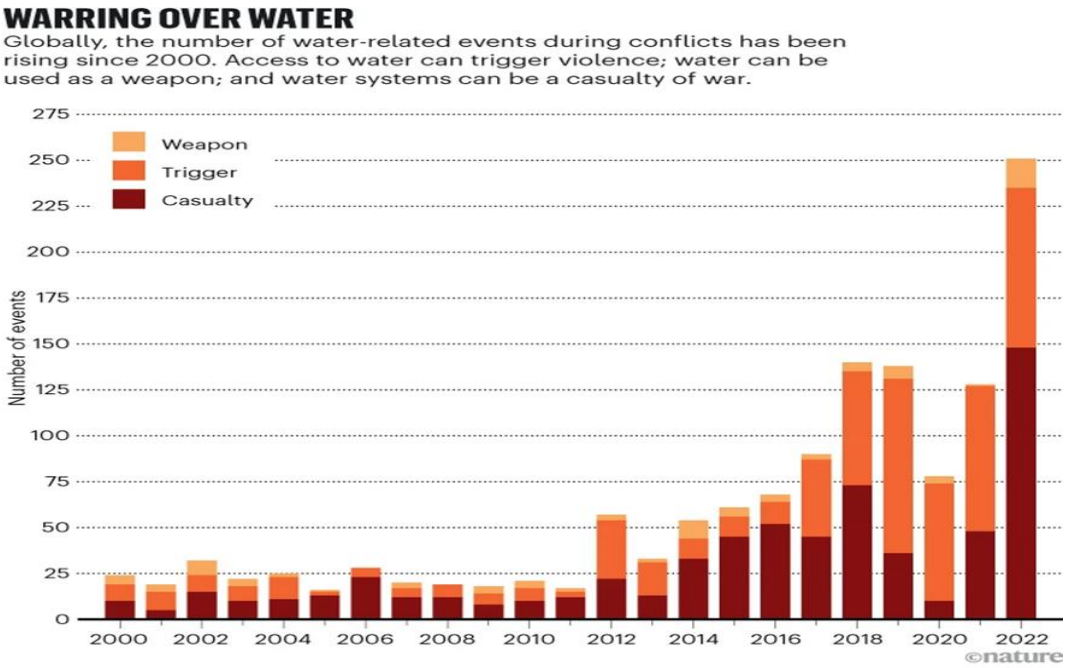
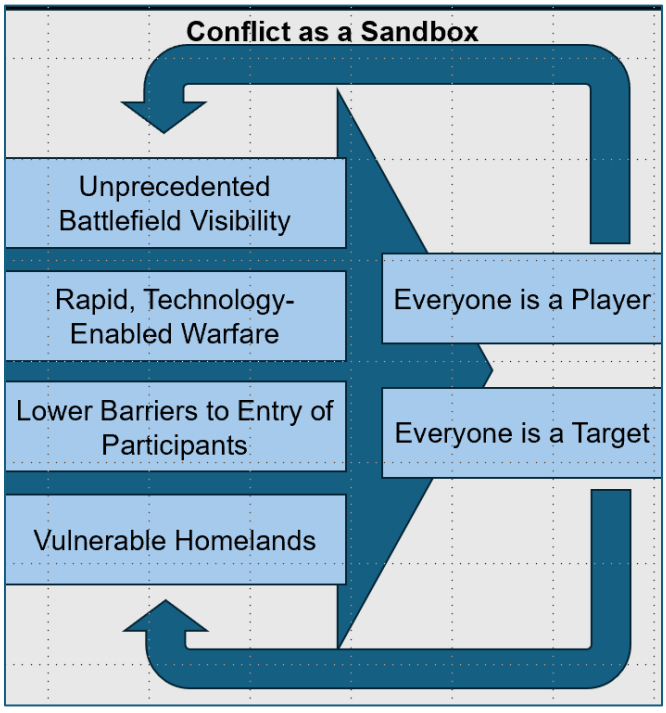


Figure 5 Image depicts increase of water-related events. [Nature.com]

information manipulation. The compromise of data, either hacked or leaked, leads to vast volumes of data on organizations and individuals published online with unknown long-term implications.

Conflict as a Sandbox



The future dynamics of warfare are highly likely (71-85%) to be shaped by the concept of "conflict as a sandbox." This environment allows for the minimally restrictive application (testing) of new or immature strategies, concepts, and capabilities by militaries, the private sector, or citizens, thus impacting the trajectory of any conflict.

Conflict as a sandbox offers indirect participation into conflict, without direct escalation, and offers a testbed environment for countries and businesses to participate, often without loss of life or "boots on the ground." This truly creates a future where everything is visible, everything is targetable, everyone is available, and everyone is accessible.

Drone Swarm Advancements Likely to Disrupt Enemy Forces By 2035

Executive Summary

Drone swarms will likely (56-70%) disrupt enemy forces more effectively by 2035 due to technological developments, decreasing barriers to entry, and application flexibility. Despite a lack of an established doctrinal foundation, military commanders at the tactical and operational levels will take advantage of drones to disrupt and destroy enemy forces on future battlefields. The deployment of multiple drones or swarms, made possible through low-cost options, will increase lethality while limiting risk to personnel.

Discussion

Sophisticated software, improved battery performance, and increased payload capacities make battlefield drones more useful and lethal. Drone swarm formations improve these capabilities by multiplying the effects. “Swarm Intelligence is the principle that a group of simple intelligences operating in concert can operate as a single, collective intelligence with superior capabilities to any of the individuals.” [H] This capability enables a single operator to control several separate drones by only making inputs as if they were a single machine. The amplification of an operator’s capability will reduce the overall personnel requirements for delivering drone effects. [H] The swarm could prioritize and continue executing missions as elements of the swarm are destroyed. [H] Another advantage of swarm applications is overwhelming countermeasures by saturating airspace with a high enough volume to outnumber adversary capabilities.

Decreasing barriers to entry in drone utilization opens this capability to anyone. Lowering costs of systems and equipment, low-tech maintenance and parts kits, and little to no experience required to operate a drone make them ideal to implement in almost any conflict. [H] Many of the drones in use on today’s battlefield are civilian drones. They are not very durable and relatively inexpensive. Most smaller drones also do not require a robust infrastructure to integrate and operate in a fight. [H] Cheaper drones are more expendable, so an operator does not expect them to last very long or

Figure 6 AI Generated Image using ChatGPT showing how Drone Swarms will enhance existing capabilities on the future battlefield. ChatGPT

have to invest in many additional parts or expensive maintenance capabilities. [H]

Military forces currently utilize thousands of drones in various applications, creating tactical flexibility. Drones proved useful against traditional targets in the Azerbaijan and Armenia conflict when Azerbaijan's UAVs obliterated Armenia's robust ground-based air defenses and then systematically destroyed Armenia's ground force equipment, including tanks, artillery pieces, and supply trucks. [H] Ukrainian and Russian forces are extensively experimenting with new applications for drones, such as loitering munitions. This drone capability includes single-use drones, which hover above a target before diving into it and exploding with it. [H] Overall, drones are a cost-effective system that provides an agile and responsive capability to commanders willing to use them. [H]

Analytical Confidence

The analytic confidence for this estimate is *medium*. The solo analyst has limited experience with the subject and a short period of time for research and analysis. Numerous sources exist, but they are not all from reliable sources with corroborating information. There is general agreement among sources that indicates rapid development on this subject, but the analyst did not use a structured method to create more depth in the assessment. Additionally, this report is likely to change with new information and expected technological developments, given the lengthy time frame of the estimate.

Author: LTC Joseph Bell

Use of Networked Acoustic Sensors for Integrated Air Defense Almost Certain by 2035

Executive Summary

Integrated air defense systems using networked acoustic sensors to detect and eliminate small Unmanned Aerial Vehicles (UAV) are almost certain (86-99%) to be employed by 2035 due to the proven success in Ukraine, availability of existing acoustic systems, and survivability compared to radar systems. Despite the limited effective range of acoustic systems, this provides capable early warning when it is too risky to turn on traditional radar systems.

Discussion

Ukrainians reinvigorated networked acoustic sensors; a solution used before the age of radar in their air war with Russia. By establishing a network of thousands of microphones across the country, Ukrainian forces can locate incoming Russian UAVs such as the Iranian-made Shahed-136. [H] Before the development of radar, many countries, including the United States, used acoustic sensors to detect incoming aircraft. Like those early warning systems, the Ukrainians use these acoustic sensors to direct their anti-air artillery assets toward the attacks, increasing the chances of destroying the UAVs before reaching their target. [H]

Figure 7 Marine Corps Light Marine Air Defense Integrated System. National Defense Magazine

For over two decades now, police forces deploy acoustic sensor networks to pinpoint the location of shooters or snipers. [H] The US Army Research Lab even developed the Unattended Transient Acoustic MASINT Systems (UTAMS), using similar technology to locate the point of origin for mortar rounds shot at US service members. [H] Coalition forces use the information from UTAMS to either direct counter-battery artillery fire or to vector quick reaction forces to the location in the hopes of capturing the people shooting indirect fire at friendly forces. By modifying the UTAMS software, US forces could quickly retrofit the systems to detect UAV noise signatures. These systems might even detect enemy stealth aircraft that can fool traditional radar systems because of their radar-absorbing properties.

One problem with traditional active radar systems is that they emit high-power radio waves during operations, which makes it simple for enemies to locate the radar system using radio direction finding. Because of this risk, radar installations are usually high-priority targets as part of the Suppression of Enemy Air Defenses (SEAD) during the

early stages of combat. The US military developed the Army Long-Range Persistent Surveillance (ALPS) and Marine Expeditionary Long-Range Persistent Surveillance (MELPS) to minimize this threat. [H] These passive systems do not emit their own electromagnetic radiation. Instead, they use sources like AM/FM radio stations or other radio sources already existing in the operating environment to detect aircraft. [H]

Analytical Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LtCol Erik Keim

Blending in the Electromagnetic Spectrum Highly Likely to Decrease Probability of Detection and Interception of Communications by 2030

Executive Summary

It is highly likely (71-85%) that militaries will blend with civilian transmission instead of relying solely on specific military electromagnetic spectrum by 2030 due to the availability of Software Defined Radios (SDRs) and the proven success of digital camouflage. Despite the military's strong cultural bias to only use reserved military spectrum, the risk of easy detection will necessitate the use of civilian frequencies.

Discussion

Figure 8 AI Generated Image of Ukrainian Forces using direction finding to locate Russian units. Ask Sage

Software-defined radios (SDRs) break free from traditional radios' hardware limitations by using software to adjust their operating frequency bands. This allows SDRs to function across a much wider spectrum range compared to their hardware-restricted predecessors. [H] By leveraging software-defined radios (SDRs) for radio direction-finding techniques, the Ukrainian military tracks Russian communications, enabling them to pinpoint the location of both command-and-control nodes and even individual unmanned aerial system (UAS) operators. [H] Commercially available software-defined radios (SDRs) revolutionize Ukrainian communications intelligence by enabling a single device and antenna to scan the entire spectrum, detecting Russian communications across all potential frequencies, unlike traditional radios which required dedicated equipment for each band. [H] Upon pinpointing Russian forces with SDR technology, Ukrainians unleash devastating attacks, employing a lethal arsenal ranging from traditional mortars and artillery to cutting-edge rocket-propelled systems and even first-person drones. [H]

Ukrainian forces are using a combination of electronic decoys as well as techniques to blend in with commercial communication networks to reduce the risk of detection by Russian Forces. [H] Traditional military radios broadcast on reserved frequencies with much higher power than commercial transmissions, making it easier for the adversary to distinguish between military and civilian transmitters. [H] Using the same frequencies as

commercial products like Bluetooth, Wi-Fi, 4G, and 5G networks allows forces to digitally camouflage their transmissions. [H] While standard camouflage prevents the enemy from quickly seeing your location by blending in with the environment, digital camouflage in the electromagnetic spectrum achieves the same end-state by blending in with civilian transmissions in that area.

Lacking modern radio equipment with transmission encryption, Russian forces in occupied areas of Ukraine find themselves susceptible to radio jamming and eavesdropping. [H] Ukrainian jamming tactics have rendered traditional Russian single-channel radios ineffective, forcing Russian forces to resort to unreliable communication methods like commercial radios and even cellular phones. By using these less secure systems, the Russians make it easier for Ukrainians to listen in on their unsecured communications. [H]

Analytical Confidence

The analytic confidence for this estimate is moderate. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LtCol Erik Keim

Space-to-Cellphone Likely by 2030: Revolutionizing Military Communications

Executive Summary

Space-to-cellphone connectivity is likely (56%-70%) to be available for military use by 2030 due to numerous companies deploying satellite constellations with this capability. Despite current military commanders' attempts to reduce or eliminate electromagnetic transmissions and minimize the enemy's ability to locate their forces using radio direction finding, Space-to-cellphone connectivity's flexibility and increased lethality will drive its adoption.

Discussion

In January 2024, Starlink tested its Direct to Cell (DTC) service, which allows standard mobile phones to send text messages over their satellites without needing traditional ground-based cellular towers. [H] DTC service uses the traditional 4G LTE mobile standard, so a unique receiver is not required to use the service. Following a successful test, Starlink initiated operations by partnering with mobile service providers in eight countries: the United States, Australia, Canada, New Zealand, Japan, Switzerland, Chile, and Peru.

This initial launch focuses on text messaging services, but the company plans to expand globally in 2024 with voice, data, and Internet of Things (IoT) capabilities following in 2025. Military personnel on the battlefield will benefit from significantly faster data transmission back to command centers, with upload speeds ranging from 7-18 Mbps. [H] This enables quicker sharing of critical information like high-resolution images, sensor data, and even live video feeds, potentially enhancing situational awareness and decision-making for troops.

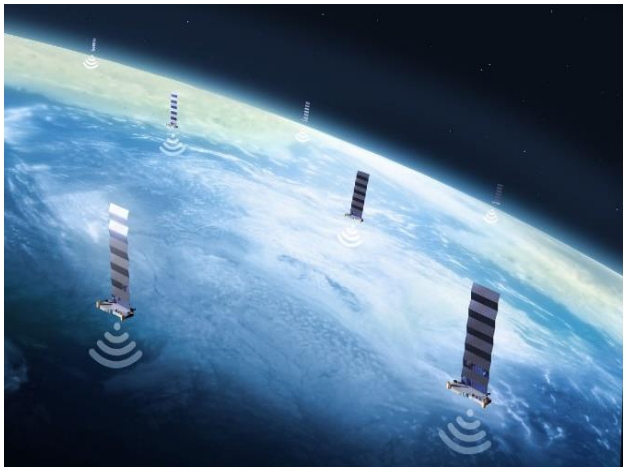


Figure 9 Depiction of Starlink satellites. Live Science

In February 2023, China Satellite Network Group challenged Starlink's dominance by announcing plans to launch a competing constellation of 13,000 satellites in Low Earth Orbit (LEO). They aim to establish a competing global internet service with its LEO satellite network. Experts see this constellation as an attempt to counter Elon Musk's influence and potentially disrupt Starlink's operations. [H] DTC represents a threat to the Chinese Communist Party's control of information since it could allow Chinese citizens to access uncensored online information outside of their government-controlled Internet. Ren Yuanzhen, a researcher

with the Beijing Institute of Tracking and Telecommunications, suggested that the Chinese satellites should have methods to perform soft and hard kill of other satellites in space.

Analytical Confidence

The analytic confidence for this estimate is moderate. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LtCol Erik Keim

Virtual Deception Will Almost Certainly Drive a Shift in Intelligence-Sharing Strategies by 2030

Executive Summary

Virtual deception will likely (86-99%) reshape intelligence-sharing protocols with allies and partners by 2030. The rise of intelligentized warfare may necessitate policies emphasizing closer collaboration and rapid information exchange. However, the purpose of intelligence sharing diminishes if allies and partners do not contribute, discern actionable information from deception, or continuously improve sharing practices. While challenges might arise, large-scale combat operations may necessitate sharing sensitive information with all coalition partners to mitigate the trust erosion sophisticated disinformation campaigns can achieve.

Discussion

In 2011, the United States developed the Afghan Mission Network to share information necessary for complex operations involving 48 North Atlantic Treaty Organization (NATO) and Partner Nations. The concept required the evolution from a need-to-know to a need-to-share culture. [H],[H] However, this was likely (56-70%) before the information evolution of intelligentized warfare, where deep fakes may quickly shape an alternate reality.

Figure 10 Per Forbes, "Deepfakes are videos or images that often feature people who have been digitally altered, whether it be their voice, face or body, so that they appear to be "saying" something else or are someone else entirely." Forbes

During large-scale combat operations (LSCO), security cooperation (SC) will likely need to extend beyond trusted partners categorized in security agreements such as the Five Eyes (FVEY), the Quad, or NATO's Enhanced Opportunities Partner. [H] A RAND study of Iraq and Afghanistan security cooperation identifies that trusted partners continue to have communication systems and classification issues. Adversaries will likely exploit these through virtual deception operations, especially with non-trusted partners operating within degraded agreements or networks. [H] For instance, Russia disseminated a deepfake video of the Ukrainian President instructing his nation to surrender, and Ukraine infiltrated Russian television to broadcast a deepfake of the Russian President declaring martial law in response to a supposed Ukrainian invasion. [H] However, such tactics become problematic when allies not privy to the deceptive strategies are integral coalition members. [H]

Intelligence sharing is unlikely (31-45%) to be beneficial unless all partners are contributing and able to differentiate actionable intelligence from deceptive information. Using Distributed Ledger Technology (DLT), non-trusted partners (e.g., countries, companies, and nonstate actors) can use everyday technologies to participate in collaborative intelligence networks. DLT is a systematic, encrypted, tokenized blockchain technology that ensures secure, immutable, and verifiable transactions and data sharing; when deep fakes occur, allies share information. [H] For example, blockchain technology is becoming more popular in supply chains, healthcare, real estate, and digital identification businesses. Developers use blockchain technology in digital assets (i.e., cryptocurrency). [M] By sharing intelligence and deception tactics with partners, a unified force multiplies its effectiveness in the complex information battlespace.

Regulators and policymakers, however, are highly likely (71-85%) to counter that existing security frameworks are adequate and that resource constraints in many countries limit their ability to analyze and protect intelligence. Additionally, they may argue that DLT technology is still an emerging technology with scalability challenges and security vulnerabilities. [M] Finally, they may emphasize that democracies with free media inherently check the spread of misleading information through open debate, and that disinformation is not as prevalent as some claim.

Despite these challenges, modern warfare occurs simultaneously in the physical and virtual worlds. During large-scale combat operations, the effectiveness of coalitions will depend on trust, intelligence, collaboration, and shared resources working towards a common goal. Successful multinational collaboration relies on mutual understanding and security agreements between the participating nations. This underscores the complexity of securing coalition operations, where coalitions must balance diplomatic and operational considerations against security requirements. [M]

Analytic Confidence

This analysis has a *medium* level of confidence. The author carefully evaluated sources using established tools (Trust Scale and Web Site Evaluation Worksheet); however, additional limitations influenced uncertainty. First, the lack of in-depth knowledge of security agreements and frameworks might lead to misinterpretations or oversimplifications of complex security implications. Second, instead of conducting solo analysis, collaborative perspectives could strengthen understanding. Third, a structured analytical process, which guides critical source evaluation, was not employed. Finally, international relations and future technology advancements introduce inherent unknowns due to potential shifts in power dynamics and technological advancements. To mitigate the identified limitations, advanced artificial intelligence platforms, like Perplexity and Gemini, aided in open-source content research and editorial support.

Author: LTC Michael “Neal” Miller

Nations Almost Certainly Will Use Lethal Autonomous Weapons System in Combat by 2035

Executive Summary

Lethal autonomous weapons systems (LAWS) use on the battlefield is almost certain (86-99%) before 2035 due to adaptive automation technology, great nations' unwillingness to agree to legally binding international agreements, and the efficiency and precision of technology. Despite concerns with civilian risk, accountability, an arms race, and proportionality, usage is likely inevitable since lethality can vary, autonomy is indistinguishable, nations have constrained resources and the existential threat of large-scale combat operations (LSCO).

Discussion

Many societies, knowingly or unknowingly, routinely accept and use automation, artificial intelligence (AI), and robotics daily. They purchase computing devices, limited memory machines such as generative AI or self-driving cars, and robots in stores, observing them daily on media platforms or using them at work or play. Each technology has levels of automation of decision and action selection. [H]

Table 1 Levels of Automation of Decision and Action Selection	
High	10. The computer decides everything, acts autonomously, ignoring the human
	9. informs the human only if it, the computer, decides to
	8. informs the human only if asked, or
	7. executes automatically, then necessarily informs the human, and
	6. allows the human a restricted time to veto before automatic execution, or
	5. executes that suggestion if the human approves, or
	4. suggests one alternative
	3. narrows the selection down to a few, or
	2. The computer offers a complete set of decision/action alternatives, or
Low	1. The computer offers no assistance: human must take all decisions and actions.

Figure 11 Simple four-stage model of human information processing. ResearchGate.net

Currently, militaries classify weapons systems as human-in-the-loop (HITL; machine gun), human-on-the-loop (HOTL; semi-autonomous weapons; Phalanx Close-In Weapon System), and human-out-of-the-loop (HOOTL; LAWS) and operate in the land, air, sea, and space domains. [H] As automation ascends from HITL (Level 1 (Low)) to HOOTL (Level 10 (High)), human engagement reduces, and autonomy increases. Given this, nations may classify semi-autonomous weapons systems as levels 2-8 since a commander or operator can be involved in the lethal decision. Militaries often fail to consider a system's size, purpose, or capabilities, each with benefits and costs, when determining automation level. However, they are likely (56-70%) to use this to justify the utilization of lethal autonomous weapon systems (LAWS). Given this, it is highly likely (71-85%) that a nation will quickly transition to levels 9-10 through adaptive automation during an existential threat like LSCO, especially using LAWS technology as a countermeasure. [H]

Great power nations cite several reasons for not supporting or abstaining from legally binding international agreements (e.g., United Nations (UN) *Convention for Certain*

Conventional Weapons (UN-CCW), UN Group of Government Experts on LAWS) that limit LAWS usage on the battlefield.

- Russia does not limit military use of artificial intelligence or robotics, stating that control and oversight should remain with the state. [H]
- The United States (US) outlines the usage of autonomous weapon systems (AWS), stating that International Humanitarian Laws (IHL) already exist concerning distinction, proportionality, and precautions. [H,H]
- China is intentionally ambiguous in its position, violating its commitment to the UN-CCW by publishing the AIDP while using IHL challenges to limit other nations' positions. [H]
- The UK and France use clarifying language to state their AWS position. [H,,H]
- Countries with limited technological development capabilities overwhelmingly favor legally binding instruments. [H]

While the unsuccessful use of a LAWS in Libya in 2020 raised ethical concerns, the 2020 Nagorno-Karabakh War showcased that drones are a tactical tool, an evolution of technology. [H]However, compared to manned aircraft, drones' low cost, simplicity, and availability could revolutionize the strategies of nations with weaker or non-existent air forces. Throughout the campaign, the Azeris exploited Armenian air defense mistakes, emphasizing that anti-drone equipment can deter the effectiveness of armed unmanned aerial vehicles (UAV). For example, small drones can slip through air-defense capabilities, but their small size restricts the weaponry they can carry. Despite drones providing Azeris an air advantage, heavy ground fighting was necessary to win the war. [H] Lacking air forces, actors like Azerbaijan, Armenia, and Hezbollah will turn to drones. Nations with sophisticated industrial bases, like Turkey, Russia, and Iran, are highly likely to deliver adaptive automation solutions despite civilian risk or concerns with ethical issues, driven by a desire to gain valuable feedback on operational capabilities in battlefield environments. [H]

The development and use of LAWS creates ethical and religious controversy. Critics argue that deploying unproven technology in unpredictable situations raises the risk of civilian casualties and creates accountability concerns. Additionally, LAWS could trigger

Figure 12 Despite drones providing Azeris an air advantage over Armenia during the 2020 Nagorno-Karabakh War, heavy ground fighting was necessary to win the war. Caliber.az

an arms race and lead to endless debates about proportionality and the ethics of second-strike systems. While acknowledging potential benefits, critics worry about ethical boundaries and propose controls. These range from a complete United Nations ban to a code of conduct requiring human oversight, reflecting the belief that humans should retain ultimate responsibility for killing. Proponents, however, argue the sufficiency of existing international law and a total ban could hinder beneficial applications like collaborative combat aircraft and unmanned ships (e.g., No Manning Required Ships (NOMARS)). [H]

Analytic Confidence

This analysis has a *medium* level of confidence. While we carefully evaluated sources using established tools (Trust Scale and Web Site Evaluation Worksheet), some limitations influenced uncertainty. First, the author lacks specific expertise in political science, potentially impacting the interpretation of complex political implications. Second, I conducted the analysis solo, lacking collaborative perspectives that could strengthen understanding. Third, a structured analytical process, which guides critical source evaluation, was not employed. Finally, this technology's global scale and long-term timeframe introduce inherent unknowns due to potential shifts in power dynamics and technological advancements. To mitigate these limitations, we aided open-source content research with advanced AI platforms like Perplexity and Gemini, which provided valuable information and editorial support.

Author: LTC Michael “Neal” Miller

Rapid War-Time Innovation Required to Compete and Win in 2030 and Beyond

Executive Summary

Rapid and continuous war-time innovation is highly likely (71-85%) to influence the outcome of conflict in 2030 and beyond due to continuous advancement in technology and adjustments in tactics during conflict. Despite the Department of Defense's (DoD) increasing rhetoric and focus on innovation, the DoD may not be prepared in 2030 and beyond.

Discussion

Figure 13 Ukrainian soldiers with a truck retrofitted by Car4Ukraine: Business Insider

Militaries continually find ways to combat advanced technologies through low-cost tactics or equipment solutions. Ukraine, with a smaller military, weaker capabilities, and a smaller economy, blunted a Russian invasion and countered several Russian attacks due to their rapid war-time innovations in equipment, capability, and tactics. [H] Their military rapidly innovated in numerous ways including their use of European pick-up trucks both as improvised missile-systems and as a tactic to confuse Russian snipers. [H,H] Since the driver and passenger seats are reversed, Russian snipers targeted a cement filled dummy in the passenger seat instead of the Soldier. Adding these to the passenger seat confused Russian snipers, causing them to aim at the dummy instead of the driver. [H]

The technological advantage that Western militaries have enjoyed may not exist in 2030. Adversaries will continually challenge systems and tactics through low-cost solutions. An Iranian drone strike in 2024 on US Soldiers in Jordan demonstrated potential innovative techniques to combat high-tech Western capabilities. This drone tactic, whether coincidence or intentional, approached undetected by tailing a US drone. [H] As technology becomes more readily available, multiple actors and nations have access to technological advancements and low-cost solutions. [H] With strains on defense budgets, adversaries that focus heavily on defense spending, and the availability of technology to all actors, it is likely they may surpass western militaries in some technologies. [H]

To combat this, service members on the ground must have the ability to make timely decisions, recommend adaptive and innovative approaches, and have the flexibility to

quickly implement new ideas. [H] Rapid, war-time innovation is essential to adapt and overcome future conflicts. It is not possible to predict the capability of current advancements in future conflict with certainty. However, a change in culture that offers the freedom and flexibility to innovate are imperative to future success. Quick implementation timelines and less risk-averse environments are equally necessary. It currently takes incredibly too long to provide new technology to a warfighter. [H] Leaders must be comfortable with testing new tactics or equipment and balancing this risk. Peacetime innovations are often too costly to sustain. Focusing on a culture of innovation that embraces experimentation, agility, learning, and balanced risk, may improve the outlook for 2030. [H,H]

Analytic Confidence

The analytic confidence for this estimate is *moderate.* Sources were very reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Given the extended time horizon of this estimate, this report is sensitive to emerging information. To mitigate the identified limitations, advanced artificial intelligence platforms, like Perplexity and Gemini, aided in open-source content research and editorial support.

Author: LTC Kristine M. Hinds

Free Space Optics are Highly Likely to Ensure Reliable, Secure Communications in Future Conflicts by 2035

Executive Summary

Free Space Optics are highly likely (71-85%) to be used in future conflicts by 2035 due to recent development and testing and the vulnerability of traditional cable and radio communications. Despite the potential degradation of capability from weather and other conditions, the technology will provide vital capability in a denied or degraded electromagnetic environment expected in near-peer competition.

Discussion

Fiber optic cables use thin strands of glass or plastic to carry light pulses, whereas Free Space Optics (FSO), on the other hand, transmits data through the air or space without any physical media. FSO systems use infrared lasers to transfer data securely and covertly without using physical cabling or detectable radio transmissions. They are extremely difficult to disrupt since the adversary must place an object directly in the line of sight between the transmitters. Additionally, an enemy would need to place equipment within 12 meters of the beam just to intercept the laser transmission, making them much more secure than traditional radio transmissions. [H] The data rates for FSO links are about 100 gigabits per second, about a thousand times higher than typical satellite communication links, making them a feasible alternative to physical links.

Figure 14 Image shows the comparison of signal dispersion between laser and microwave Effect Photonics

More than 12 major companies are bringing this technology to market, with L3 Technologies, Anova Technologies, Fog Optics, Laser Light Communications, LaserOptronics, and LightPointe Communications – all key players. [M] In May 2022, Mitsubishi Electric Corporation announced that it had developed the world's first operational ground-to-space laser communication terminal, opening the possibility of using FSO for satellite communications. [M] Experts estimated the 2021 market at just under USD1 billion and forecast it to grow to USD14 billion by 2031. [M]

Figure 15 Okinawa Marines Test FSO Defense.gov

Over the last decade, the Marines experimented with FSO to replace microwave-style communications systems. Since 2018, they tested the systems' ability to support ground-to-ground and ship-to-ground missions in various environments, including areas in and around the South China Sea, proving the ability to support military operations. [H] In the past, long-distance laser communication was highly susceptible to degradation due to atmospheric conditions such as temperature, wind, air pressure, and humidity. Companies recently developed new technology to ensure laser quality even in complex atmospheric conditions. [H]

Along with the more highly televised drone and missile attacks aimed at international shipping, Houthi rebels recently cut three major communication cables that run under the Red Sea. [H] Accidental damage from fishing, shipping, earthquakes, and other incidents disrupts nearly 200 undersea cables around the world each year. [H] It is expected that during a conflict with the United States, many adversaries will attack these undersea cables to disrupt the command and control of US and allied forces. [H]

Analytical Confidence

The analytic confidence for this estimate is moderate. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LtCol Erik Keim

Machine Learning Likely to Boost Interoperability in US-Allied Defense Strategy Before 2030

Executive Summary

Machine learning is likely (56-70%) to improve interoperability in United States (US)-Allied battle networks before 2030, driven by budget shortfalls, the evolving nature of global threats, and the increasing global arms market. Dissimilar platforms and security agreements are likely to complicate and restrict data sharing. Despite these challenges, the strategic shift towards countering long-term competition with China and Russia will likely require new, revised, and expanded agreements that enable real-time data sharing necessary for combined battle network integration.

Discussion

Military defense strategies, almost certainly (86-99%), will benefit from integrating battle networks with allied and partner nations. Currently, integration is unlikely (31-45%) due to the diversity of intelligence, surveillance, and reconnaissance (ISR) sensors and defense platforms, as well as policy limitations and concerns. [H]

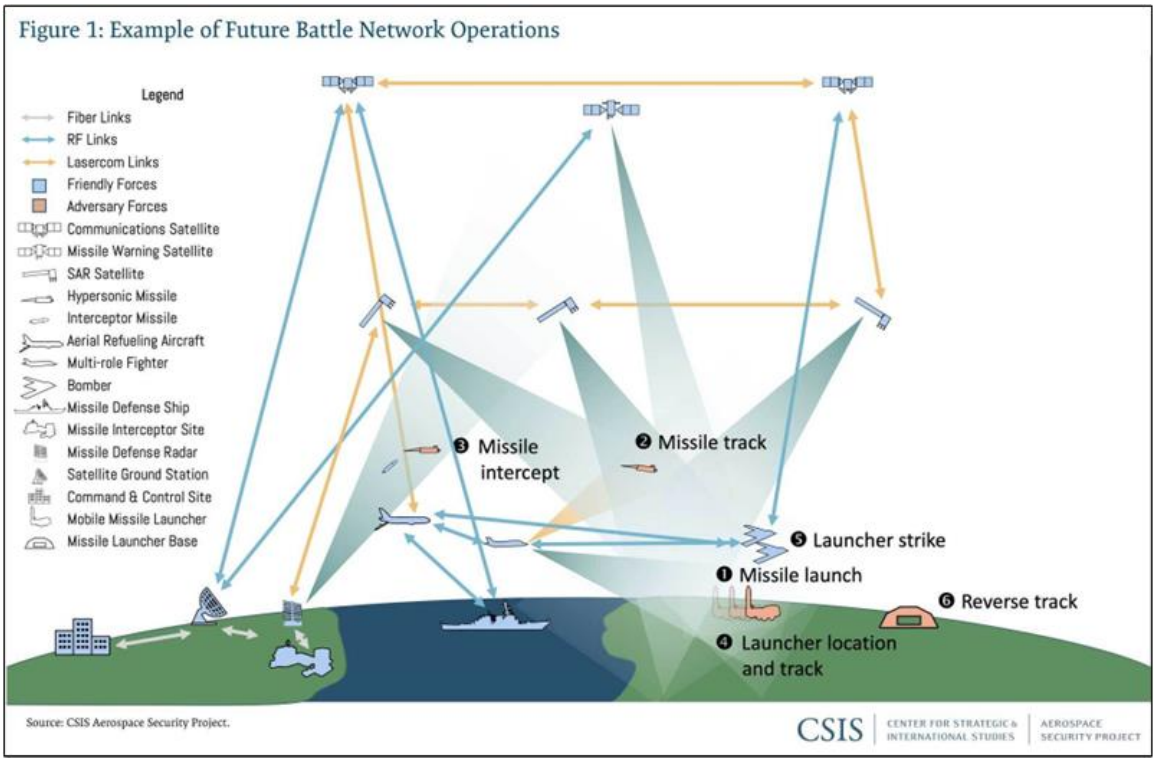


Figure 16 Machine language will likely connect battle networks between ally and partner sensors by 2030. CSIS

Military operation and support (O&S) costs dominate nation-state budgets, constraining modernization opportunities. [H] Strategic offset analysis will likely convey an adversary's advantage due to a faster-growing economy and the ability to field a larger and more capable military. [H] The global arms market, once dominated by five countries, now includes 23. This expansion has led to a more significant number of incompatible

platforms. [H] However, leveraging a network of allies and partners' ISR sensors and defense platforms will likely reduce the effect of these challenges.

Machine learning will highly likely (71-85%) offer a secure, real-time bridge between incompatible electronic sensors and equipment, enhancing military capabilities while adhering to policies and solidifying alliances. [H] Meta's open-source TransCoder system migrates code with self-supervised neural translation. The artificial intelligence system translates code between languages without needing pre-existing translated examples (parallel data). Currently, TransCoder can translate functions between C++, Java, and Python 3. Its self-supervised approach translates between different programming languages (e.g., COBOL to C++) even when large data sets of code are scarce. TransCoder can modernize legacy codebases by translating them into more efficient and maintainable languages. [M] Similarly, IBM and Google have generative artificial intelligence tools that assist clients in updating legacy code to modern languages. [H]

Widespread adoption between dissimilar platforms and technologies will highly likely challenge implementation timelines. Security agreements like Five Eyes and The Quad, foreign military sales (FMS) interests, and intelligence policies will almost certainly further complicate and restrict data sharing. However, information-sharing postures continue to shift from "need to know" to "need to share" to improve interoperability, as demonstrated in the Afghanistan Mission Network [H] and NATO Partnership Interoperability Initiatives. [H] Many nations cannot leverage alliances as an offset strategy; however, battle network integration furthers shared interests and FMS is not the only solution.

Analytic Confidence

This analysis has a *medium* level of confidence. The author carefully evaluated sources using established tools (Trust Scale and Web Site Evaluation Worksheet); however, additional limitations influenced uncertainty. First, the lack of in-depth knowledge in hardware design, language modeling, and intelligence-sharing constraints might lead to misinterpretations or oversimplifications of complex technical implications. Second, instead of conducting solo analysis, collaborative perspectives could strengthen understanding. Third, a structured analytical process, which guides critical source evaluation, was not employed. Finally, diplomacy, international relations, and intelligentized warfare introduce inherent unknowns due to potential shifts in power dynamics and technological advancements. To mitigate these limitations, we aided open-source content research with advanced AI platforms like Perplexity and Gemini, which provided valuable information and editorial support.

Author: LTC Michael "Neal" Miller

Use of Autonomous Semi-Submersibles for Logistics Resupply Missions Likely by 2035

Executive Summary

The United States will likely (56-70%) use autonomous submersible vehicles for logistical resupply of remote military units by 2035 due to technological advances, recent successful test deployments, and the number of organizations developing vessels for navies around the world. Despite US decision-makers' resistance to using autonomous vehicles in warfare, recent experimentation, and the need to covertly resupply forces will drive the adoption of unmanned systems.

Discussion

Facing the high risk of deploying surface vessels, the US Navy turned to submarines for clandestine resupply missions in 1942. [H] Drug trafficking organizations exploit semi-submersible craft for clandestine drug shipments into the United States, a tactic they've adopted for over the past decade. [H] The US Coast Guard struggles to detect and intercept these craft due to their propulsion systems, size, and the materials used in their construction. [H] The continued use of submarine technology for the secret delivery of material and supplies is almost certain (86-99%), given the past success and decreased risk to the shipper of the goods.

Figure 17 Unmanned surface vessels Ranger and Mariner sail alongside Japan's Mogami-class frigate JS Kumano on Sept. 27, 2023. MC2 Jesse Monford/U.S. Navy

The US Navy ramped up its unmanned vessel program by deploying four prototypes across the USINDOPACOM area of operations, marking a successful deployment of over 45 thousand nautical miles. [H] During the experimentation, they tested emerging concepts and developed maintenance estimates for the various platforms. Refined by naval experimentation, these concepts are highly likely (71-85%) to evolve into doctrine for manned-unmanned collaboration at sea within the next 5-10 years.

Defense contractors, including Anduril Industries and Cellula Robotics, are developing multi-mission unmanned submarines for the Royal Australian Navy. [H] These vessels can have higher endurance and can operate at depths beyond those of manned submersible craft because they do not need to accommodate human crew space in their designs. The

number of firms developing large form-factor unmanned submersibles makes it highly likely that multiple militaries will have this technology in the next 5-10 years.

Analytical Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LtCol Erik Keim

Ethical and Legal Dilemmas Likely to Impact Lethal Autonomous Weapon System Usage in 2030 and Beyond

Executive Summary

Ethical and legal dilemmas are likely (56-70%) to impact the speed and usage of lethal autonomous weapon systems (LAWS) during potential conflicts by 2030 due to concerns over human dignity, national and international policy, and lack of attribution for unintended consequences. Despite strategic leader debate and adversaries' continued investment in the technology, nations do not have a clear consensus on the definition of LAWS and remain divided on its prohibition.

Discussion

Contemporary conflicts involve the use of autonomous systems, most notably in Ukraine and Russia, using autonomous air systems, greatly increasing the effectiveness of indirect fire capabilities. [M] Western nations are highly likely to utilize fully autonomous lethal systems in future conflicts. [H] US defense professionals debate the use of LAWS for various reasons, including the overall ethics and morality involved. One argument, "Prohibitionism," asserts that using LAWS is inconsistent with human dignity, calling for its prohibition. [H] This is due to the lack of human involvement when identifying targets for lethal action, without human involvement. In contrast, "Restrictionism" acknowledges the concerns raised by prohibitionists but argues that LAWS can also protect human dignity if its use meets certain criteria. [H] This criterion includes:

- The action is militarily necessary.
- The action involves a distinction between combatants and non-combatants.
- The action does not target noncombatants for harm.
- All incidental harm to non-combatants is minimized.

Other debates compare LAWS to weapons of mass destruction, and they contradict ethical and moral values. Others argue that the only moral answer is to embrace and utilize autonomous weapons. If the US faces adversaries with these capabilities, it would be immoral and of detriment to US security and servicemembers, to not reciprocate in kind. [H] These ethical debates over human

Figure 18 A sign attached to a robot from the Campaign to Stop Killer Robots, a coalition of non-governmental organizations opposing lethal autonomous weapons or so-called 'killer robots.' CFR

dignity and morality are not likely to dissipate over the next few years. While the US continues to consider and advocate for guidelines for usage, many nations advocate for full prohibition. [H]

Humanitarian organizations compare LAWS to the use of anti-personnel landmines, highlighting policies that subsequently banned landmines. [H] Similar policies do not exist for LAWS and are unlikely to develop due to vastly different opinions and lack of any agreed upon definition. [H] The US does not support a ban on LAWS, nor does it prohibit their development or usage, but current policy is very ambiguous with room for interpretation. Department of Defense Directive (DODD) 3000.09 outlines that systems must allow for "operators to exercise appropriate levels of human judgement" and that "adequate training and doctrine" remain available. [H] Words like "appropriate," "human judgement" and "adequate" leave wide openings for multiple interpretations. Without clear guidance, operators may be hesitant to employ such systems without understanding the policy or ethical impacts.

Adversaries do not face the same weariness with autonomous weapons use. Russia opposes a legal ban on LAWS and emphasizes that decisions for usage must remain with individual states. [H] While it is not likely that Russia used fully autonomous weapons in Ukraine, they have the intent to explore this technology, making it possible for the future. [H] The People's Republic of China's stance of LAWS lacks clarity due to varying definitions of LAWS. Publicly, China endorses legally binding actions, but they have a narrow definition compared to others. [H] This allows China to pursue the technology without reaching their definition on the topic. [H] Even if select adversaries choose not to employ the technology, they may still conduct arms sales with US adversaries, with less concern for the usage. [H]

There is significant concern over the lack of attribution when using LAWS, raising concerns over accountability. Due to their autonomy, they have the potential to act unpredictably, possibly leading to unlawful or immoral actions. This leaves a responsibility gap where the system acts immorally but cannot hold a human accountable because it is genuinely unclear if anyone was truly responsible. [H] Various organizations took a stance on this. The European Parliament states that "autonomous-decision making should not absolve humans of responsibility" and the UN Group for Government Experts states "human responsibility for decisions on the use of weapons systems must be retained since accountability cannot be transferred to machines." [H] There is still no national or international consensus on attribution. Until servicemembers understand the responsibility behind development and usage, employment of LAWS may fall behind that of adversaries.

There is overall concurrence that the US will have fully autonomous weapons within the next five years, but insistence that they will always involve humans. [H] The US may take this stance now, but it is unlikely that all adversaries will do the same.

Analytic Confidence

The analytic confidence for this estimate is *high.* The author carefully evaluated sources using established tools and sources tended to corroborate one another. Limitations influenced uncertainty in this confidence rating. The author has a lack of in-depth knowledge on lethal autonomous weapons which may result in oversimplifications of complex technology. Additionally, instead of conducting solo analysis, collaborative perspectives could strengthen understanding. To mitigate the identified limitations, advanced artificial intelligence platforms, like Perplexity and Bard, aided in open-source content research and editorial support.

Author: LTC Kristine M. Hinds

North Korea’s Artificial Intelligence Capability Growth Highly Likely by 2027 and Beyond

Executive Summary

The Democratic People’s Republic of Korea (DPRK)'s artificial intelligence (AI) and machine learning (ML) technologies across various sectors are highly likely (71-85%) to increase in capability by 2027 and beyond. This is due to the state’s strong support for AI/ML development, the country’s global AI/ML advancement, the focus on sensitive applications, and the intangible transfer of technology (ITT). Despite the perception by many nations that the DPRK is a backward nation, its technology progresses and presents a danger to the world through sophisticated cyberattacks and autonomous weapons systems deep within the world's infrastructure.

Discussion

The DPRK supports AI and fosters its growth. [H] The development of its “Eunbyul” AI program in 1998 marked the beginning of the country’s journey into AI. [H,H]
The Eunbyul AI program was developed to address nationwide challenges, including forecasting air pollution levels, drought preparedness, and monitoring hydro turbine vibration. The DPRK amended the Socialist Constitution in April 2019 to include “informatization” as a core economic effort. This reflects the state’s emphasis on developing AI/ML as part of an “informatized/digitized economy” alongside self-reliance, modernization, and scientization. [M, H]

During the COVID-19 pandemic, the country applied AI/ML to create a model for evaluating proper mask usage and prioritizing clinical symptom indicators of infection. The country invented its voice recognition software called Ryongnamsan by employing deep-learning algorithms; it functions similarly to voice recognition programs like Apple's Siri, Amazon's Alexa, and Google's Assistant. [M] The country continues development and promotes AI/ML technology across various sectors which keeps the DPRK interwoven in the world's progress and enables forays into fields such as wargaming and surveillance. [H,H,M]

The country’s researchers have applied AI/ML for sensitive military applications, including wargaming and surveillance. They have also continued scientific collaboration with foreign scholars. [M] Examples of AI/ML studies for potential military applications include research on topics like computer vision, natural language processing, and reinforcement learning. [M] While hardware procurement for AI development may be challenging due to sanctions, Supreme Leader, Kim Jong-un, actively seeks to keep pace with global progress by leveraging open-source information and scientific collaboration.

In 2013, the DPRK established its Artificial Intelligence Research Institute (AIRI) under the Bureau of the Information Industry Guidance. Eight years later, the North Korean Ministry of Information Industry incorporated the AIRI under its control in an explicit

action to enhance its technological capabilities. This move indicated high state support and funding for these efforts. [H]

The technologies will likely play an increasingly critical role in the country's diplomatic, information, military, and economic structures. China and the DPRK invest heavily in similar technology and research and development (R&D). Even though China might not need the country for R&D there is evidence that the two are sharing research. [H,H] This presents an opportunity to exploit North Korea and China's intertwined automation and decision-making capabilities, i.e., attack one to impact the other.

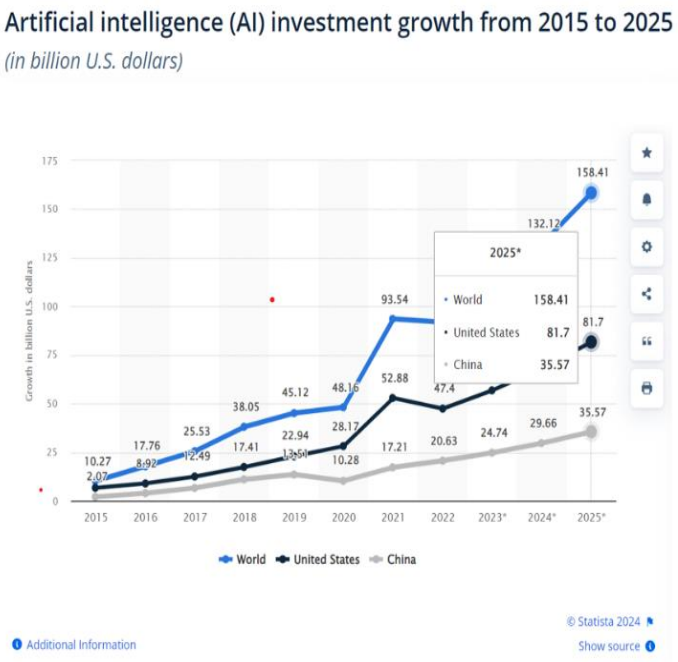


Figure 19 AI Investment. Statista.com

One danger is the continued progression and extension into cyber warfare. AI will play an increasingly important role in the country's technological landscape. [H] There is evidence that the country plans to use AI/ML for more sophisticated and effective cyberattacks. [M,H] DPRK's software-centric technology because it is transferrable by intangible means, i.e., ITT. Autonomous weapons systems and their integration into global infrastructure pose unpredictable risks. [M,M,M]

Analytical Confidence

The analytic confidence for this estimate is *moderate*. Overall, sources received high trust scores and tended to corroborate one another. However, the analyst worked alone, chose not to use a structured method, and limited himself to unclassified research. Furthermore, given the volatile, uncertain, complex, and ambiguous (VUCA) operational environment in the East Asian region, this report may change due to new information. Significant investment from our adversaries' and competitors' governments and private sectors could change this report's forecast. Additionally, an unpredictable leap in technology could skew this report's prediction.

Author: COL John E. Cooper

Quantum Computing Highly Likely to Revolutionize Military Logistics Before 2035

Executive Summary

Quantum computing deployment on the battlefield is highly likely (71-85%) before 2035, driven by the complexity of logistics and supply chain data analysis and challenges presented in contested environments. However, transitioning this technology from the lab to the real world faces significant hurdles due to its high resource demands and potential to disrupt international stability. Though legislation aims to establish a quantum development sandbox, building quantum-compatible logistics frameworks offers an asymmetric advantage over adversaries.

Discussion

Quantum computing will almost certainly (86-99%) address complex problems that currently exceed the capabilities of today's computers. It achieves this by leveraging the principles of quantum mechanics to process information in new ways. [H] International corporations, like IBM, Honeywell, Google, Intel, and Cambridge Quantum, are actively exploring quantum computing, investing in application development across diverse fields

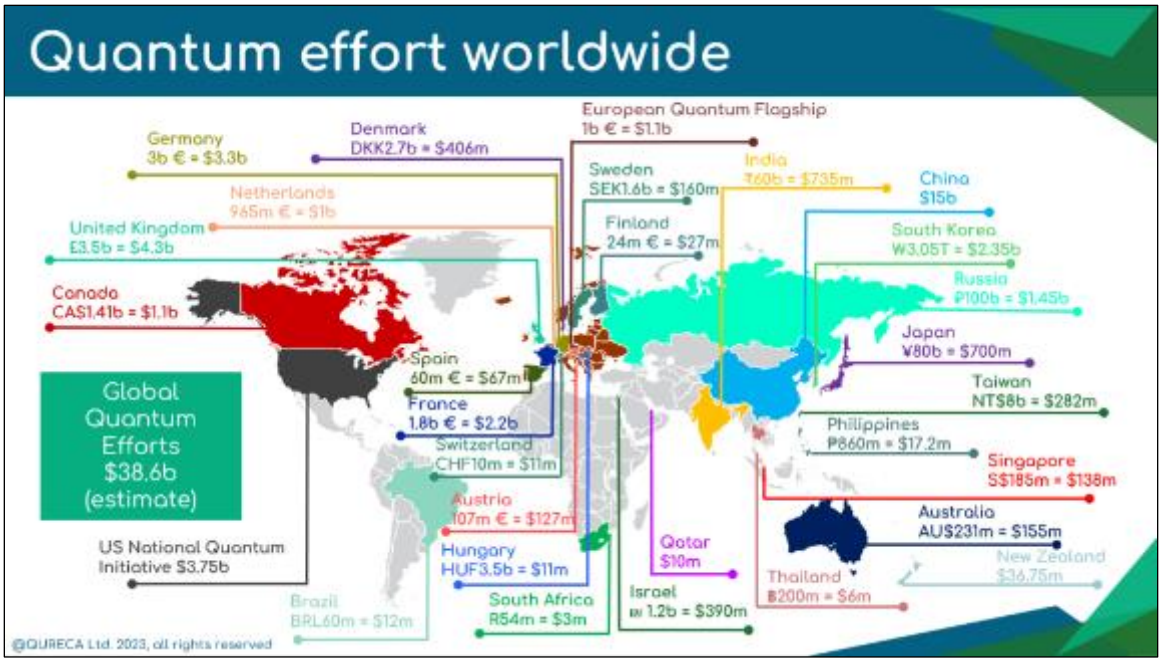


Figure 20 The global technology market is projected to reach $106 billion by 2040. Qureca.com

like drug discovery, material science, financial modeling, and logistics management. [H] Quantum computing's data processing capabilities are almost certain (86-99%) to significantly change logistics and supply chains, enabling real-time optimization of purchase, storage, transportation, and delivery systems to warfighters. Quantum computers leverage quantum bits, or qubits, to achieve the same tasks. Unlike regular bits confined to 0 or 1, a qubit can be both simultaneously with varying probabilities for each

state. Imagine a maze – a regular computer would explore each path one by one until it stumbles upon the exit. A quantum computer, in contrast, tackles all paths simultaneously, pinpointing the solution much faster. This translates to superior speed, the ability to store more information, and lower energy consumption. [H] Honeywell Quantum Solution is working with vehicle producer BMW - officially known as Bayerische Motoren Werke Aktiengesellschaft - to streamline its supply chain by efficiently focusing on a complicated number partitioning algorithm to distribute diverse car parts to plants worldwide. [M]

The Department of Defense (DoD) faces challenges like those of BMW but with an added layer of complexity: adversaries equipped with advanced ISR systems and high-precision weaponry constantly threaten delivery and storage methods. This adversary actively seeks to pinpoint and destroy DOD's transportation networks and storage facilities using high-precision weaponry. A recent West Point study analyzes the Russo-Ukrainian war, highlighting logistics' decisive role in military success. [H] The study examined four hypothetical Russian offensive scenarios, exposing a critical vulnerability: insufficient vehicles to deliver essential supplies and sustain operations. The study emphasizes that militaries must continually evaluate and identify new supply routes to minimize service disruptions, especially when logistics becomes a high-value target. While the application of quantum computing in logistics remains early in development, its potential to optimize equipment delivery, especially during complex scenarios like Large Scale Combat Operations (LSCO), holds significant promise. This potential stems from its ability to analyze vast datasets encompassing suppliers, warehouses, routes, and relevant environmental factors with unprecedented efficiency and accuracy.

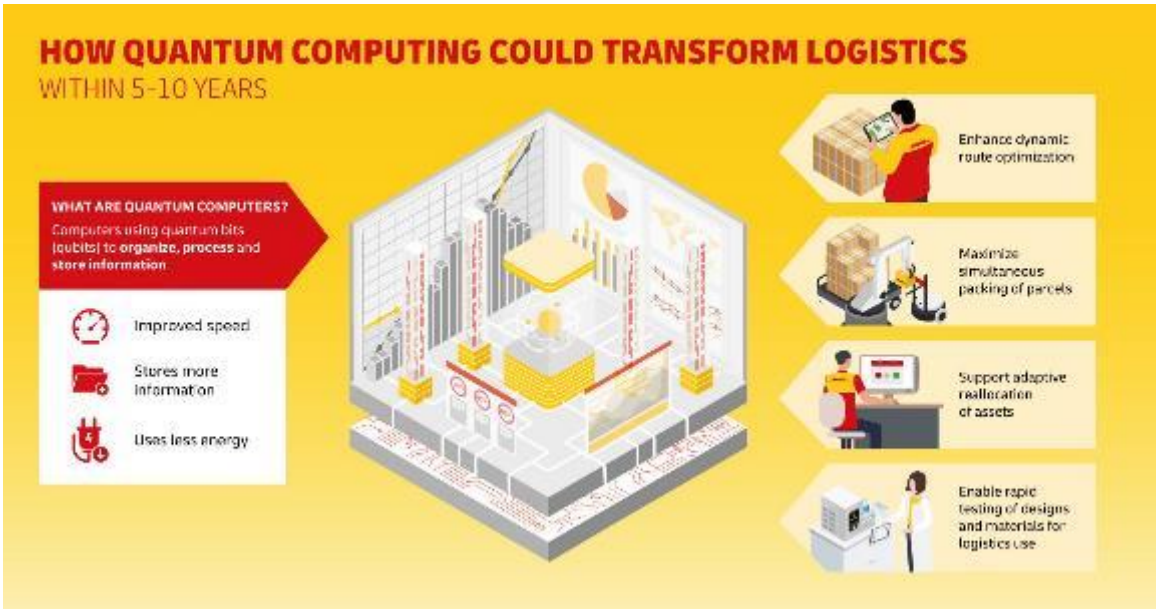


Figure 21 Strategically, quantum computing is the next frontier in military logistics and operational efficiency. DHL

While international companies continue developing real-world quantum technology applications, significant challenges remain. Firstly, quantum technology is on track but still in its infancy. Secondly, current systems require specialized environments, such as near absolute zero (-273°C), severely limiting their deployability. Lastly, it could become a potent weapon, allowing nation-states to dominate their adversaries by breaking encryption, predicting strategic decisions, and gaining information dominance. [H] Despite these challenges, the United States has authorized $1.2 billion in funding over five years [H] through the National Institute of Standards and Technology, the National Science Foundation [H] and the Department of Energy [H] for research and development. Quantum technology's potential is recognized by Congress as indicated by the United States House of Representatives (H.R.) 2739 bill, the *Quantum Sandbox for Near-Term Applications Act*. [M]

Analytic Confidence

This analysis has a *medium* level of confidence. The author carefully evaluated sources using established tools (Trust Scale and Web Site Evaluation Worksheet); however, additional limitations influenced uncertainty. First, the lack of in-depth knowledge in advanced science and engineering might lead to misinterpretations or oversimplifications of complex technical implications. Second, instead of conducting solo analysis, collaborative perspectives could strengthen understanding. Third, a structured analytical process, which guides critical source evaluation, was not employed. Finally, this technology's global scale and long-term timeframe introduce inherent unknowns due to potential shifts in power dynamics and technological advancements. To mitigate these limitations, we aided open-source content research with advanced AI platforms like Perplexity and Gemini, which provided valuable information and editorial support.

Author: LTC Michael "Neal" Miller

Private Sector Involvement in Future Conflicts Highly Likely to Increase Success by 2027

Executive Summary

Private sector companies are highly likely (71-85%) to play a significant role in the success of future conflicts by 2027 and will require inclusion and consideration in war planning and preparation by friendly forces. This is due to private company involvement and support in cyber-defense, advanced imagery, and communication that will increase the ability to support partners and allies from geographically separated locations. Despite the lack of policies and procedures for applying private sector products and services, the United States and Western allies rely on the private sector for future success.

Discussion

The Russia-Ukraine War demonstrates the importance of private-sector companies during conflict. The Atlantic Council Scowcroft Center for Strategy and Security labeled the private sector and their sphere of activities as a "sixth domain" for consideration in future war planning. [H] Private sector companies provided significant capabilities such as cybersecurity, information technology, advanced imagery, and increased communication that enabled the Ukrainian continued defense. With the rapid and continued advancements in technology, Russia's heightened frequency of cyber-attacks during the invasion resulted in minimal disruption. [H] Ukraine's cyber defense capabilities were successful due to the involvement of international private sector companies and partners for the "collective defense" of Ukraine. American tech companies, Palo Alto and Microsoft, contributed to safeguarding data and protecting Ukrainian networks by setting up firewalls, protecting critical infrastructure, and safeguarding Ukrainian data through migrating the data to foreign servers. [H] The UK Foreign, Commonwealth and Development Office (FCDO) sponsored a program enabling Ukrainian agencies to access the services of commercial companies. This arrangement paved the way for the UK government to use commercial cybersecurity capabilities when required. [H]

The continued impact by and requirement for private sector cybersecurity involvement will continue to increase through 2030. Cybersecurity is one of the fastest-growing professions and projected to grow by 35 percent by 2031. [H] Private-sector salaries are 20-35 percent higher than public sector, drawing a larger pool of talent. [H] To compete and succeed in the cyber domain in 2030 and beyond, militaries will need to leverage the private-sector's expansive talent and technology base. The North Atlantic Treaty Organization (NATO) already recognizes the need for stronger integration with the private sector, as outlined in NATO 2030, through harnessing civilian innovation and engaging with academia. [H]

Several tech companies provided other capabilities to Ukraine, such as satellite imagery and communication equipment. Amazon and Google assisted in migrating critical

Figure 22 Maxar satellite image of the southern end of a large Russian convoy near Antonov Airport near Kyiv, Ukraine, February 28,2022. Fox News

Ukrainian data to distributed cloud servers and providing technical support. [H,H] Maxar Technologies provided satellite imagery at the onset of the invasion, showing a 64-kilometer Russian convoy headed to Kyiv. They continued to provide imagery disproving Russian claims and depicting the extent of damage across Ukraine. [H] Other companies, such as Scale AI, provided images, free of cost, of recently bombed buildings and cities, allowing for accurate humanitarian and medical response to impacted areas. [H] The commercial satellite imagery industry provides greater integration with allies and partners as these images are unclassified and can be freely shared. 2027 and beyond will require greater cooperation with partners and a variety of available information in a contested space domain. Private sector imagery will likely become critical during future conflicts to enhance flexibility, information sharing, and rapid decision-making.

The private sector, labeled the sixth domain, requires consideration and inclusion in warfighting plans in preparations for the US and its allies to succeed in future conflicts. [H] Private involvement is not without concern or issue. Without regulation, private companies make decisions that directly impact the outcome of a conflict. SpaceX, responsible for providing Starlink to the Ukrainians, denied satellite internet service to prevent a Ukrainian drone from attacking a Russian naval fleet. [H] This decision demonstrated the power of one individual, Elon Musk in this case, in directing the course of a specific engagement during a conflict. Private companies may continue to make decisions that shift the direction of a conflict as they fit their requirements or beliefs. Conversely, any over-regulation or government involvement may deter private-sector

involvement altogether. To harness the private sector influence in 2027 and beyond, militaries must prepare for their involvement and include the impacts of the sixth domain in all planning.

Analytic Confidence

The analytic confidence for this estimate is *high.* Sources were very reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Given the extended time horizon of this estimate, this report is sensitive to emerging information. To mitigate the identified limitations, advanced artificial intelligence platforms, like Perplexity and Bard, aided in open-source content research and editorial support.

Author: LTC Kristine M. Hinds

Cyber Attacks on Industrial Critical Infrastructure Highly Likely to Impact Military Mobilizations by 2035

Executive Summary

Cyber-attacks on critical infrastructure are highly likely (71%-85%) to impact military mobilizations by 2035. Despite the United States' investment to protect and modernize the military's networks and critical infrastructure, civilian industrial operations remain threatened due to the increased integration of physical and digital worlds, inherently insecure software, and adversarial cyber offensive capabilities.

Discussion

Cyber-attacks against industrial operations doubled in the US annually since 2020. [H] Recent attacks targeted municipal water systems, major ports, oil and gas pipelines, and healthcare or hospital systems. [H] Significant occurrences over the last decade include the San Francisco rail system in 2016, the New York Dam in 2016 by Iran, an unnamed gas company in 2020, a water treatment facility in 2021, the Colonial Pipeline in 2021 by Russia, a Pennsylvania municipal water authority in 2023 by Iran, and various instances on hospital and healthcare systems. [H,H,H,H,H] The growth of the Internet of Things (IoT) increased the number of entry points for adversaries to find and exploit vulnerabilities in critical infrastructure. [H] These vulnerabilities pose increased risk for military mobilization by disrupting the civilian population or impacting activities on military installations, while impacting production, transportation, and communication of assets.

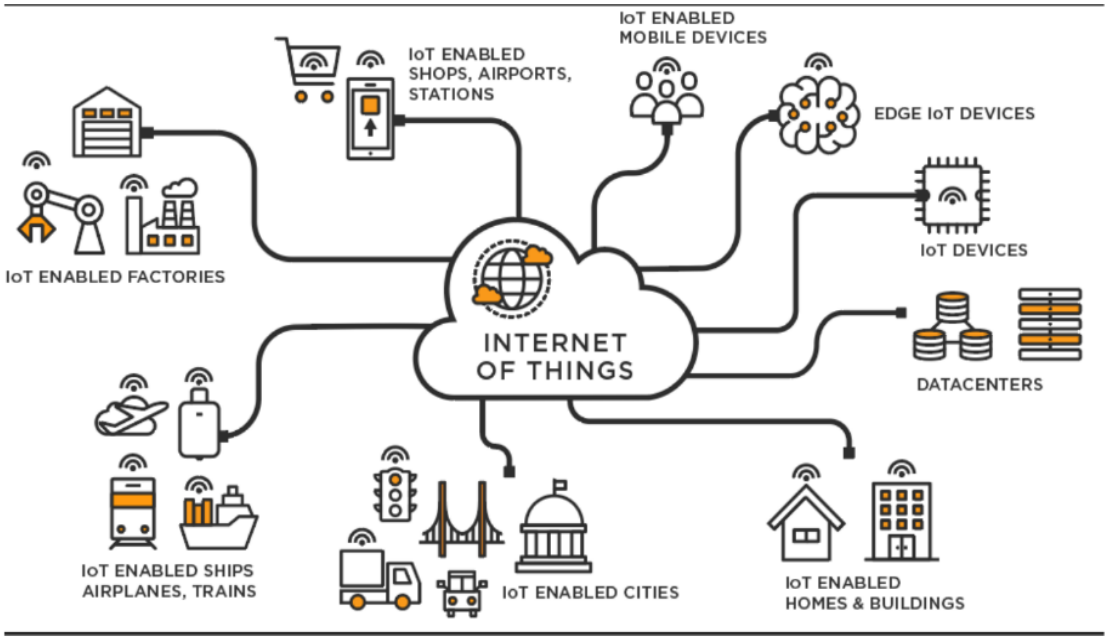


Figure 23 Displays the internet of things, network of connected devices. University of Michigan

The number of connected devices is likely to increase by 45 percent by 2030. [H] Many physical objects now have digital controls linked to core IT networks, increasing digital potential cyber targets when adversaries consider critical infrastructure weaknesses. [H] This vastly increases the required defensive space for digital devices and increases opportunities for adversaries to target critical infrastructure.

Recent warnings from the Cybersecurity and Infrastructure Security Agency (CISA), the National security Agency (NSA) and the Federal Bureau of Investigation (FBI) highlight the cyber threats by Chinese state-sponsored actors. [H] Although the People's Republic of China (PRC) is a sophisticated cyber adversary, they do not need to use sophisticated methods to break the US's critical infrastructure. The PRC leverages insecure infrastructure and weaknesses in legacy hardware and software. The Volt Typhoon hack stealthily infiltrated critical infrastructure and SOHO devices to pre-position itself for future acts of sabotage. [H,H] Other incidents, such as the Iranian hacking of municipal water authorities, were possible due to cybersecurity weaknesses and poor password security. [H] Russia's recent Fancy Bear attack targeted small home and office systems (SOHO) routers and leveraged common devices for their government's aims. [H]

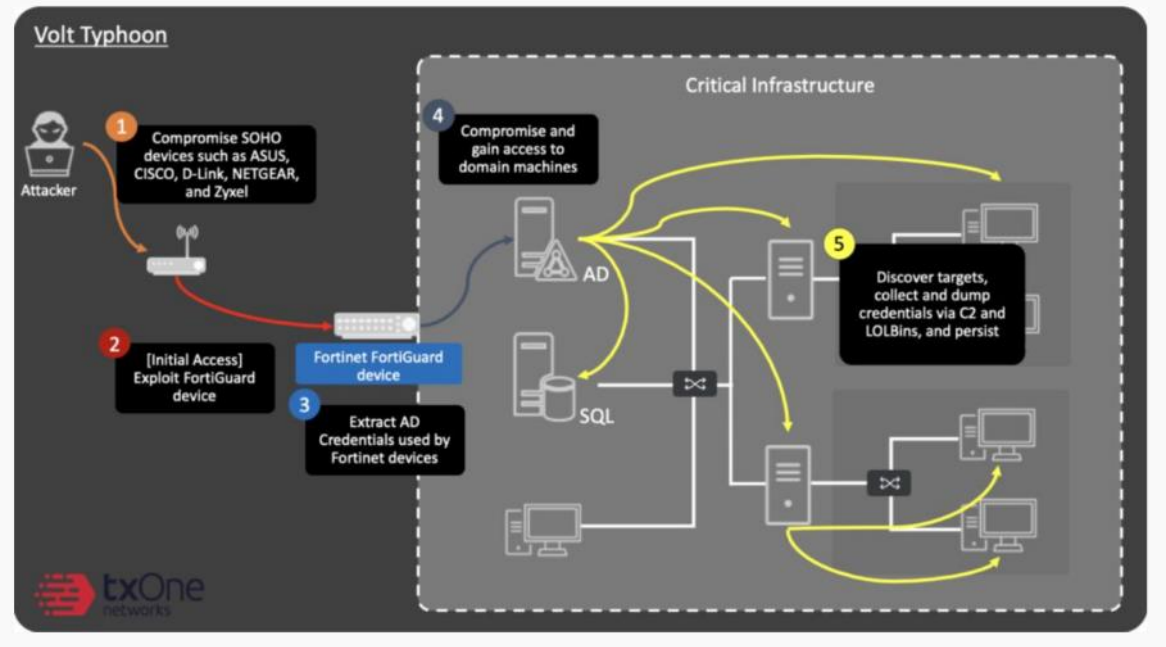


Figure 24 Flow chart of Volt Typhoon Simulated Attack. txOne Networks

The PRC, specifically, focuses on political and military targets, and on critical infrastructure to ready themselves for destructive cyber-attacks against the US and western nations. [H] The 2023 DoD Cyber Strategy also highlights the PRC's use of cyber to degrade combat capability and hinder mobilization. [H] Chinese military doctrine emphasizes the importance of the cyber domain in any conflict with the United States. [H] Chinese backed hackers accessed critical civilian infrastructure for at least the last five years, undetected, giving them considerable information on energy and water controls. [H]

It is highly likely that China will use cyber to deter the United States and de-escalate total war or conduct cyber-attacks in the event of a major crisis by 2030. [H]

Analytic Confidence

The analytic confidence for this estimate is *high.* While the author carefully evaluated sources and considered them reliable, there is likely additional information on classified networks that more thoroughly address this topic. Additionally, the author lacks specific expertise in cyber-attacks that potentially impact interpretation of material. There was adequate time, but the analyst worked alone and did not use a structured method. This report is likely to change with new information and expected technological developments, given the lengthy time frame of the estimate. To mitigate the identified limitations, advanced artificial intelligence platforms, like Perplexity and Bard, aided in open-source content research and editorial support.

Author: LTC Kristine M. Hinds

Near Even Chances that the United States Defense Industrial Base is Prepared for Large Scale Combat Operations by 2030

Executive Summary

The United States has near even chances (46-55%) that their defense industrial base (DIB) is prepared for large scale combat operations (LSCO) by 2030. Despite the US's emphasis in the DIB and role as a significant global supplier, the US may face challenges during LSCO with a near-peer due to inadequate surge capacity, challenges in output of materials and critical weapon systems, and lack of a flexible acquisition system.

Discussion

Developing, acquiring, and producing systems, munitions, and technologies to scale, challenges the DIB. During recent conflicts, the US faced challenges in supplying ammunitions to Ukraine due to supply chain issues and difficult ramping-up weapons manufacturing. [H] Although the COVID-19 pandemic impacted overall manufacturing, it only highlighted the already existing capacity problem within the US, and the impact of just in time logistics to sustained conflicts. [H] Ukraine's conflict led to a surge in demand resulting in a 17.5 percent increase in industrial production within the US defense and space sectors. [H] Certain ammunitions and weapons have only a single source for key components, highlighting the need for redundancy in production or reliance on allies and partners to produce equivalent items. [H] Additionally, with multiple requirements for systems and capabilities, coupled with changing technology, it is difficult to prioritize production with budgetary constraints. To maintain inventory, the US requires multiyear investments to meet any surge in requirements. [H]

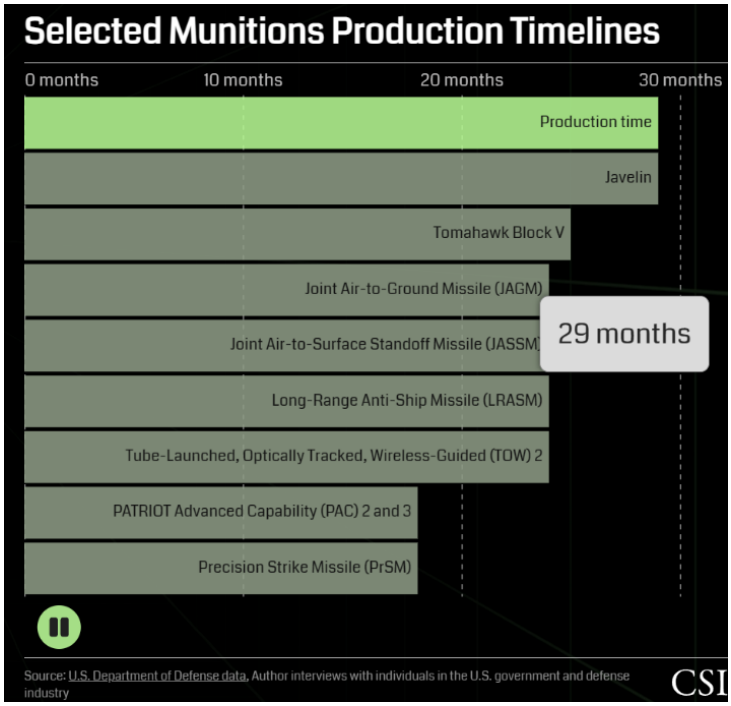


Figure 25 Image depicts munition production timelines CSIS

The Ukraine conflict highlighted the difficulty in sustaining munition requirements, especially in a protracted war. During war games conducted by the Center for Strategic International Studies (CSIS), the use of munitions during a major conflict would exceed the current stockpiles. The US would likely run out of certain munitions within one week during a Taiwan scenario. [H] They are not the only country to face this challenge.

Wargames involving the US, United Kingdom (UK) and French forces demonstrated the UK would suffer similar outcomes, exhausting stockpiles in over a week. [H]

Ukraine, while improving their DIB, recognized an opportunity to incorporate innovative technologies into their growing industrial base. [H] There was previously a disconnect between warfighters and engineers within the defense industry. However, since the mobilization of civilians within Ukraine, engineers now have military experience and can leverage this for future development. [H] Additionally, Ukraine frequently utilized commercial-off-the-shelf (COTS) products in innovative ways to address challenges within the DIB. Small tech startups assembled and distributed COTS products within weeks, which goes outside traditional defense procurement cycles. [M] These methods improve the future DIB within Ukraine, but also work around the DIB to continue supporting the conflict in innovative ways.

The US requires a resilient defense industrial base to deter conflicts effectively, specifically to compete with China, which benefits from a robust civilian manufacturing sector and a deeper pool of resources for military production. [H] The Ukraine conflict reflects the urgency of developing and maintaining a robust DIB, furthering the discussion on the status of the US's industry. Ukraine's use of COTS to bypass some of the traditional procurement cycles and highlights the need for flexible acquisition within the US. [H]

Analytic Confidence

The analytic confidence for this estimate is *high.* The author carefully evaluated sources using established tools and sources tended to corroborate one another. Limitations influenced uncertainty in this confidence rating. Instead of conducting solo analysis, collaborative perspectives could strengthen understanding. To mitigate the identified limitations, advanced artificial intelligence platforms, like Perplexity and Bard, aided in open-source content research and editorial support.

Author: LTC Kristine M. Hinds

Weaponized Water in Contemporary Conflict

Executive Summary

Hydraulic warfare is almost certain (86-99%) to influence conflict in the future due to growing dependency on water resources, increasing water stress, and remote access to water systems and infrastructure. There are numerous examples of using water as a weapon in past and current conflicts in places such as Ukraine, Gaza, and Azerbaijan. Additionally, there is increasing high water stress across most of the globe. Despite new technologies to decrease challenges associated with water security and the idea of making ecocide a fifth crime enshrined in the Rome Statute of the International Criminal Court (ICC), hydraulic warfare will become more effective and lethal as the demand for water grows and scarcity increases.

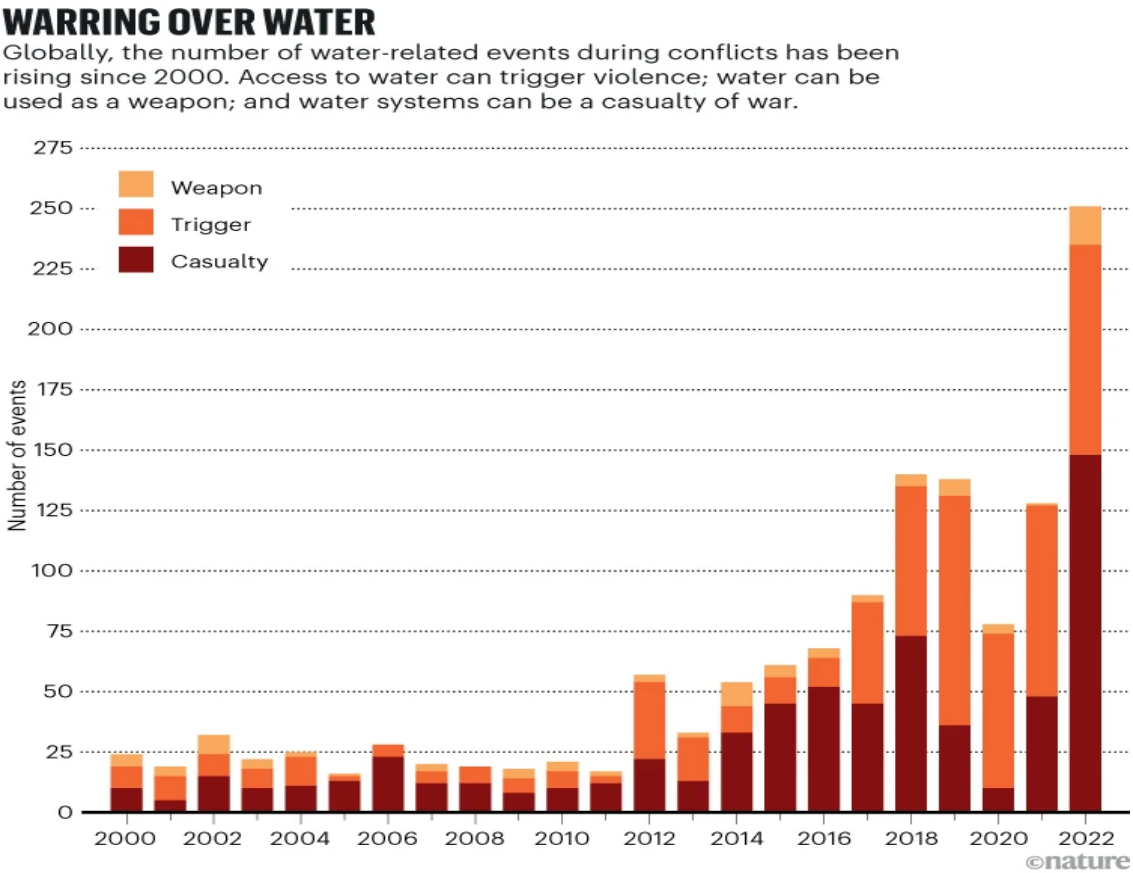


Figure 26 Image depicts increase of water-related events. Nature.com

Discussion

High water stress impacts international conflict by increasing political instability, human displacement and migration, and violent engagements. The scarcity of freshwater resources will increase tensions and the potential for conflict between state actors that depend on shared water sources. There are three distinct impacts of influencing water during conflict. The first is Direct Impact, or attacking water infrastructure as a weapon

of war. The second is Indirect Impact, where military operations harm the environment, such as poisoning water sources or contaminating soil. The third is Transboundary Impact, where the consequences are also felt in other countries. [H]

There are several current examples of water weaponization in recent and current conflicts. In the Russia-Ukraine War, Russia allegedly destroyed a dam and drained the Kakhovka reservoir. [H] This deliberate action resulted in a swollen river, creating an obstacle in southern Ukraine that allowed maneuver space for Russian soldiers. [H] There are numerous other reports of water contamination and targeting of water infrastructure. In October of 2022, Russia conducted a missile attack on civilian infrastructure in Kyiv that left 40 percent of the population without access to water. [H] As another example in Gaza, Israel is pumping thousands of cubic meters of seawater into tunnels to disrupt Hamas' capabilities. However, environmental analysts warn of ecocide and the potential damage to the aquifer that holds Gaza's groundwater that 2.3 million people rely on. [H]

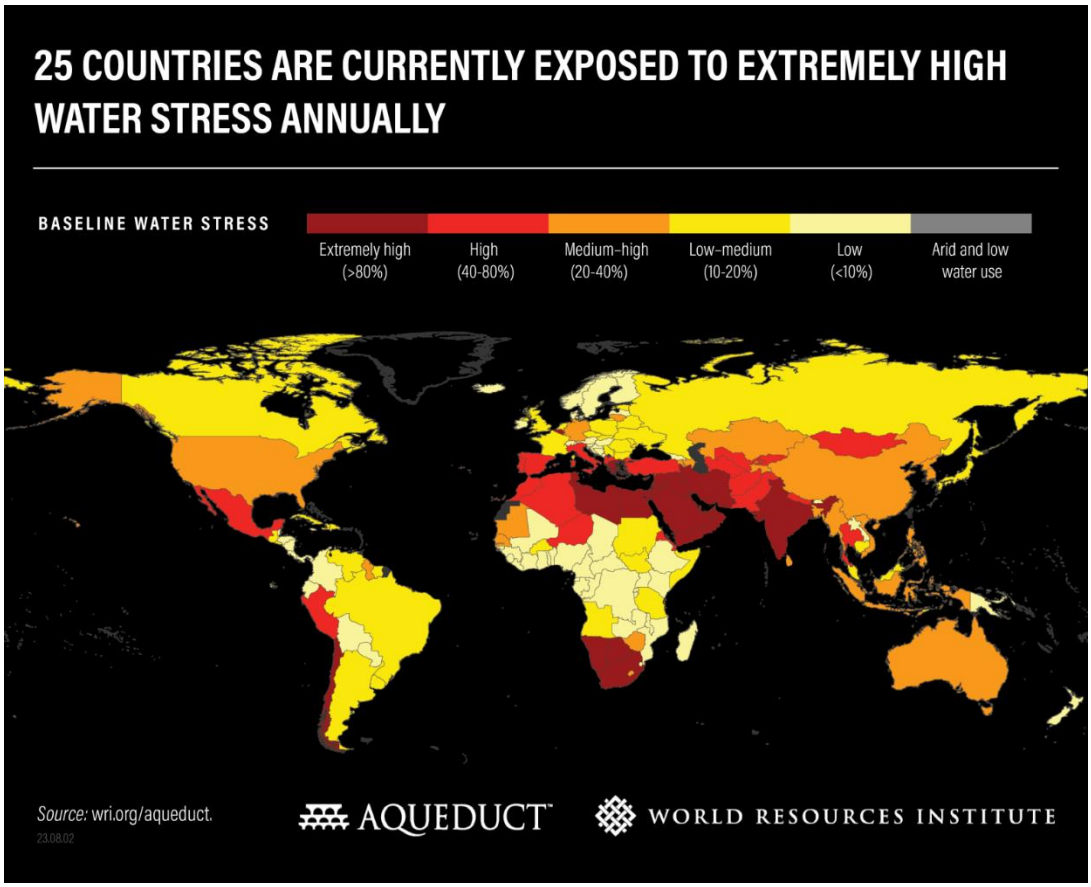


Figure 27 World View of Water Stress Impacts. World Resources Institute

Current conflicts demonstrate targeting or using water as a weapon, but increasing competition for dwindling natural resources drives threats of conflict. [H] At least 50 percent of the world's population, or four billion people, live in highly water-stressed conditions for at least one month of the year. [H] High water stress indicates a country uses 40 percent of its water supply, while extremely high water stress means withdrawing 80

percent of its renewable supply. An additional one billion people will experience extremely high water stress by 2050. [H]

Negotiations between Armenia and Azerbaijan highlight the transboundary impact of water management and its influence on conflict. Primarily considered by some as one of the reasons for the war, access and control of water have contributed to a decline in drinking and irrigation water in recent years. A country's actions in managing water sources can profoundly effect other countries living downstream or that share dependency on water resources.

Taiwan’s water struggles are another example of dependence on water as a limited resource. Agriculture and the semiconductor manufacturing industry demand an incredible amount of fresh water. As the climate changes, typhoons deliver less reliable rainfall to replenish dwindling resevoirs. [H] This high demand and dependency on freshwater leave the Taiwanese island vulnerable to hydraulic warfare from adversaries.

Analytical Confidence

The analytic confidence for this estimate is *high*. The author used reliable sources that tended to corroborate with one another. The analyst used artificial intelligence to scope the assessment and source reliable information. There was adequate time, but the analyst worked alone and did not use a structured method. Given the enduring and growing dependence on water, this report is stable against change over time.

Author: LTC Joseph Bell

Fortress Fleet Tactic Usage Highly Likely by 2035

Executive Summary

Nations with modern military capabilities are highly likely (71-85%) to increasingly use land-based fires to conduct maritime warfare through 2035 due to improving capabilities and lethality of systems and the staggering costs and challenges of developing and maintaining a capable naval force. Despite the current advantages some countries have with a blue-water Navy or robust maritime forces, the re-emergence of land-based fires with greater lethality allows other states to protect coastlines and forward operating bases, defend against naval adversaries, and influences the modernization strategies of land and maritime forces in their geographical areas. This strategy of protecting a fleet with land-based fires is known as fortress fleet.

Discussion

Figure 28 Image shows the Russian warship Moskva before it sank in April 2022 BBC

Originally, the concept of the fortress fleet applied to a naval fleet's operating, or sheltering, within the protection of a fort's big guns. [H] The fortress fleet gained more relevance in current and future conflicts despite dismissal by the influential 19th-century naval officer and historian Alfred Thayer Mahan for limiting maneuver and making commanders more defensive-minded. The US currently has blue-water navy primacy, leaving a remote (1-15%) likelihood of a threatening engagement in the open seas. Future conflicts may remain closer to land, where ground-based effects are necessary to achieve military objectives. As seen in the Ukraine/Russia War, Ukraine is optimizing limited resources and creating an asymmetric challenge to Russia. In April of 2022, Ukraine launched two missiles at the Russian flagship Moskva in the Black Sea, where it sank the next day. [H] Changing threats in the maritime environment may cause countries to focus resources on coastal defense systems, anti-ship missiles, and sea denial capabilities instead of sinking investments into naval fleets capable of sustained operations in the open seas.[H] Alternatively, countries can create a land-based defensive shield around their naval forces, ensuring operational resilience in contested waters while deterring incursion from enemy forces.

A country will have an obvious advantage in applying the fortress fleet concept to its own coastal defense strategy but improving Anti-Access/Area-Denial (A2AD) capabilities makes the fortress fleet concept transportable. A country can now build up A2AD assets

at forward-basing locations or resupply hubs that take advantage of strengths to enable joint protection and maneuver in lethal maritime environments. [H] Modern fortresses may demonstrate true joint operations by integrating intelligence support from satellites and electronic warfare while launching drone swarms or long-range anti-ship missiles. The combination of these effects can create an A2AD zone of hundreds of miles, making it more challenging to apply and mass naval forces. [H]

In the Pacific Theater, the United States may encounter unacceptable risk in utilizing a carrier strike group or other large naval assets within China's A2AD umbrella. However, developing a more robust Access, Basing, and Overflight (ABO) posture with partners and allies in the region would allow the United States to apply the fortress fleet concept abroad. Conflict within the Pacific Theater will require opposing landings of enemy forces and protecting against occupation of all points along a coast. [H] The United States, its allies and partners, and China may all have robust "fortresses," and this will change the application of naval forces as well as land-based armies in future conflicts.

Analytical Confidence

The analytic confidence for this estimate is *moderate*. Sources are generally reliable and tend to corroborate with one another. The analyst used artificial intelligence to scope the assessment and source reliable information. There was adequate time, but the analyst worked alone and did not use a structured method. This report is sensitive to change over a short time, given the fast pace of technological advancements and their creative applications in conflict.

Author: LTC Joseph Bell

North Korea’s Profit-Focused Cybercrime Capabilities Almost Certain to Increase by 2027 and Beyond

Executive Summary

The Democratic People's Republic of Korea (DPRK)’s cybercrime capabilities are almost certain (86-99%) to increase by 2027 and beyond due to its technology programs which benefitted in recent decades by its state sponsorship, centers of higher learning, focused professionals, and financial profitability. As its tech prowess develops, the country profits and again enhances its tech – this is a continuous cycle. When coupled with its citizens’ extreme loyalty and desperate economic situation, the country is a dangerous state actor. Despite its status as one of the poorest countries in the world, and weakening infrastructure, the country maintains one the of preeminent computer-based crime programs in the world. When combined with artificial intelligence (AI), potential quantum computing, and emerging technologies, the DPRK tech-based threat presents a grave challenge to the US and its allies.

Discussion

The DPRK developed its offensive cyber program over the last 35 years through domestic innovation and foreign assistance. [H] The country’s computer-related crime modus operandi underwent major transformations, shifting from disruptive computer-based attacks primarily targeting South Korean government agencies, to hacking banks and cryptocurrency exchanges located both on and off the Korean Peninsula. [H] Supreme Leader, Kim, Jong-Un’s regime ensures its societies compliance and support of the government and the military, just as his father and grandfather did since the founding of the country in 1945.

In the mid-1980s, Pyongyang established three institutions that significantly contributed to advancing the country’s offensive tech programs: Mirim College, the Pyongyang Informatics/Information Center, and the Korea Computer Center. High-scoring graduates from top technology and computer science universities serve in the country’s military and intelligence agencies to expand its electronic capabilities and readiness. It is almost certain this well-educated and hand-picked force will perpetuate.

The country commands an estimated six thousand e-crime agents through four intelligence organizations scattered across the globe. [M,H] North Korea’s tech capabilities are sophisticated and multifaceted, posing a significant threat to global cybersecurity and the international financial system. [H,H] Computer-based crimes are more efficient, cost-effective, and lucrative than Pyongyang’s past illicit activities. Given the country’s motivations, cost-benefit ratio, and low-risk of consequences, the DPRK is almost certain that the DPRK’s e-crimes will perpetuate. [M]

Recent analysis and developments in North Korean hacking suggest that Pyongyang will expand its hacking operations with increased focus in the following areas: phishing

campaigns, ransomware attacks, foreign over the counter (OTC) brokers, and decentralized finance (DeFi) platforms. [H]

The country's illicit tech strategy focuses on aggressive information collection, financial theft, and espionage, with a considerable computer-based capability targeting various industries globally. Despite being comparably small, DPRK's electronic-espionage capability is particularly active, and the country punches above its weight in cyberspace. [M] However, the country does not have free reign in the E-espionage realm. For example, South Korea actively combats the country's computer-based threats and is even expanding its research and development into its quantum capabilities as well. [L,M]

The US and its allies will pursue AI as a potential counter to the DPRK's digital threat. [H] Nevertheless, as the sophistication of AI increases, so does the complexity of cyber threats and the DPRK is aware of the advantages of AI, too. [H]

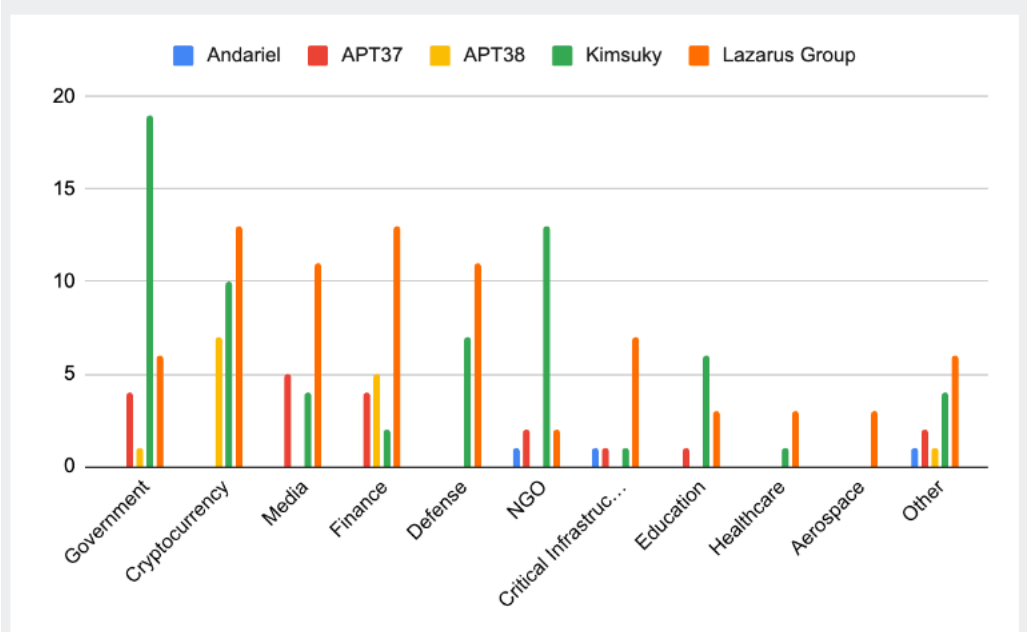


Figure 29 "Breakdown of Industry Verticals of Victims Grouped by North Korean State-Sponsored Threat Actors" Recorded Future

Additionally, there is an increasing convergence in the field of AI and cyber security because AI plays increasingly crucial roles. [M] These roles include threat detection, incident response, user verification, malicious activities prevention, and vulnerability identification. [H]

There is evidence that the DPRK is promoting the exploration and adoption of quantum computing for economic development. This is understandable given that quantum computing would demand a lesser toll on the power grid compared to supercomputers, especially given the high rate of rolling blackouts. [M]

Analytical Confidence

The analytic confidence for this estimate is *high*. While several sources received very high trust scores, other sources received a moderate trust score. Additionally, although the sources tended to corroborate one another the analyst worked alone and did not use a structured method. There are several factors which may impact the forecast of this report: the ongoing war between Russia and Ukraine; the volatile, uncertain, complex, and ambiguous (VUCA) operational environment in the East Asian region; renewed war on the Korean Peninsula; an internal collapse of North Korea; and economic development and the alleviation of poverty that lead to budget and policy shifts from military spending, cyber security, and E-frauds and intrusions.

Author: COL John E. Cooper

Foreign Investment in Land and Infrastructure Likely to Increase Vulnerabilities to National Security by 2035

Executive Summary

Foreign investment will likely (56-70%) expose more vulnerabilities to national security by 2035 due to growing influence over agricultural land, access to sensitive technologies, and critical infrastructure. Despite existing laws and regulations intended to track and control foreign investment, poor oversight and enforcement creates a lack of accountability and burdensome process, resulting in vulnerabilities for the United States.

Discussion

Agricultural land is vital for domestic food security, American jobs, and contributions to the Gross Domestic Product. Foreign investors are increasingly buying more farmland, pastures, and forestland and investing in various parts of the farm-to-table process to include water access for irrigation. [H] Food security is part of national security, and there is concern over who controls the land and other parts of our food system from seeds to meat processing and grocery store distribution. [H] Saudi Arabia (SA) owns farms in western Arizona to grow alfalfa, a water-intensive crop. These SA farms pump irrigation water from groundwater aquifers, further intensifying a water-shortage problem in the area and shipping the crops back to SA. [H] Although China is 18th on the list of foreign countries that own US agricultural land, they remain our pacing threat and a concern for their potentially nefarious utilization of land holdings. [H]

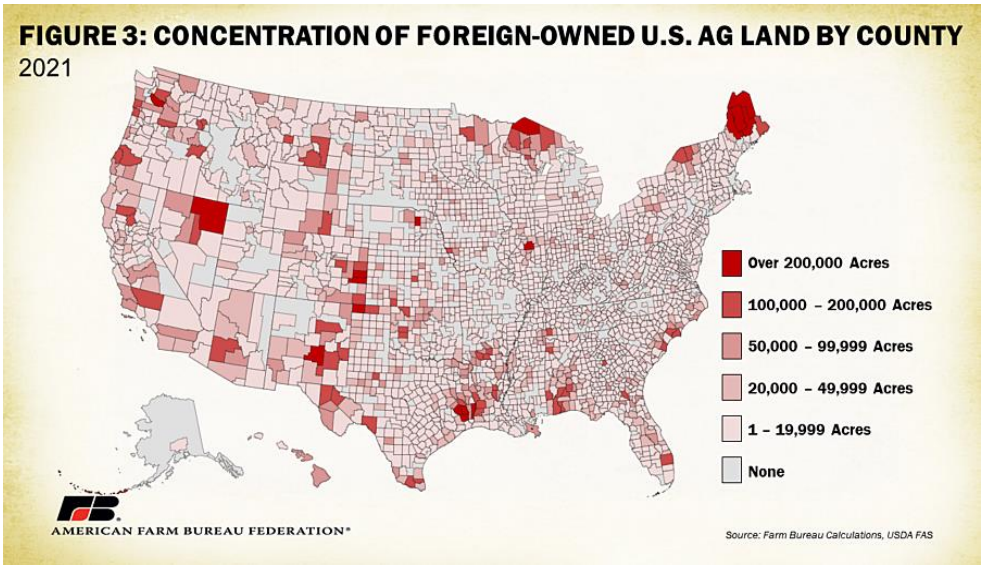


Figure 30 The image depicts the concentration of foreign-owned agricultural land across the US. Farm Bureau

President Biden said in 2022, “Some countries use foreign investment to obtain access to sensitive data and technologies for purposes that are detrimental to US national security.” [H] Mergers and company acquisitions, especially in advanced technological sectors, may

offer foreign investors access and opportunities to take advantage of sensitive technologies. In 2018, US intelligence agencies stated, “Chinese recruitment of foreign scientists, its theft of US intellectual property, and its targeted acquisitions of US firms constituted an unprecedented threat to the US industrial base.” [H]

Foreign investment also opens a window into critical infrastructure within the US by various means. In Texas, a Chinese-based billionaire purchased over 160 thousand acres of land to create a wind farm. State law intended to prevent foreigners from linking to the Texas electricity grid halted this project. [H] This incident is one example of the multiple avenues foreign investors may use to access infrastructure and public utility assets and gain access to sensitive locations. In January of 2023, the US prevented a China-based investment group from building a corn mill on land near an Air Force base in North Dakota, calling it a security risk. [H]

Analytical Confidence

The analytic confidence for this estimate is *medium*. The solo analyst has limited experience with the subject and a short period of time for research and analysis. Numerous sources exist, but they are not all from reliable sources with corroborating information. There is general agreement among sources that indicates rapid development on this subject, but the analyst did not use a structured method to create more depth in the assessment. Additionally, this report is likely to change with new information and expected technological developments, given the lengthy time frame of the estimate.

Author: LTC Joseph Bell

US Cyber Defenses and Policies Unlikely to Secure Vulnerabilities by 2035

Executive Summary

US cyber defenses and policies are unlikely (31-45%) to adequately secure system vulnerabilities across the public and private sectors by 2035 due to the total dependency on digital systems and software throughout public infrastructure and private businesses and the overwhelming vulnerability human error creates within cyber security. Despite existing laws, policies, incentives, and advisories to direct and encourage cyber security actions within public and private sectors, staying ahead of foreign attacks and intrusions into US systems will remain challenging as innovation decreases barrios to access data.

Discussion

Figure 31 AI-generated image representing US Cyber Defenses protecting against foreign attacks. ChatGPT

President Biden's administration released its National Cybersecurity Strategy (NCS) in March of 2023 in response to unrelenting data theft and infrastructure disruptions. From 2018-2023, ransomware attacks cost American businesses over USD 20 billion. Attacks on small businesses grew 150 percent over the last two years. These criminal acts went relatively undeterred in the past, with the new NCS supporting regulatory frameworks that will shift liability and create incentives for private firms to defend against critical vulnerabilities. [H] The administration is looking to push legislation to hold companies liable for failing to do their due diligence in cybersecurity.

Vulnerabilities persist at all business and government infrastructure levels and will remain a consistent threat indefinitely. Human error can account for a significant portion of threats to a system and continues as a persistent challenge. Verizon conducted an investigation into a data breach in 2023 and discovered that 74 percent of data breaches resulted from human errors. [H] Cyber security efforts in the future must consider the human element when creating technical solutions to problems. Cooperation between the government and industry is necessary to tackle cyber security challenges with all participating businesses and agencies. However, cooperation only goes so far as to encourage and complement actions between parties. There are still sophisticated security measures only the government can implement, but smaller players must do their part in basic cyber hygiene. The Center for Strategic & International Studies conducted a series

of roundtable discussions with senior government officials and senior information security executives from significant enterprises across various industries. During these engagements, a participant said, "It's impossible to stop all threats and trying to is a bad way to plan. Protecting the (most important assets, such as proprietary information) and accepting some level of vulnerability for other assets is more effective. [H] This perspective acknowledges the persistent nature of cyber threats but drives towards focusing limited resources on critical protection requirements instead of a whole system.

The US General Services Administration (GSA) is improving requirements within government systems and contracts. [H] Measures included in the Federal Acquisition Supply Chain Security Act will immediately improve the current cybersecurity posture and have continuous impacts as the GSA updates contracts with the latest requirements. Legislation directing accountability for cyber security and increasing liability will also help to rebalance responsibility and realign incentives for long-term investments. [H] Persistent and active defenses are critical, but these efforts will unlikely substantially decrease or limit vulnerabilities over time.

Years to Quantum (Y2Q) is the anticipated time when quantum computing will be able to break encryption methods, rendering them obsolete and creating a new paradigm for cyber security. [H] As Y2Q gets closer, the cyber security threats will only increase. Dimensional Research, sponsored by Cambridge Quantum, conducted a survey in 2022, finding that 61 percent of security professionals think quantum-enabled cyber attacks will be able to neutralize current encryption within 2 years versus 28 percent that think encryption technologies will be compromised within 3-5 years. [H]

Analytical Confidence

The analytic confidence for this estimate is *medium*. The solo analyst had adequate time for research and analysis. Numerous sources exist with corroborating information. There is general agreement among sources that challenges continue in the future, with no absolute path to total security. However, a lack of robust statistical analysis or a possible flawed interpretation of the finding may contribute to weaker analytical confidence. The analyst used artificial intelligence to scope the assessment and source reliable information. Given the estimate's lengthy time frame, this report will likely change with new information and expected technological developments.

Author: LTC Joseph Bell

Multilateral Exercises Likely to Outpace Bilateral Exercises Before 2035

Executive Summary

Multilateral exercises will likely (56-70%) outpace bilateral exercises before 2035 due to several factors, including increasing interconnectedness of global security concerns, strategic signaling, and confidence building. However, organizing and executing almost certainly (86-99%) becomes more complex as exercises include additional nations' protocols, procedures, languages, and cultures. Despite these challenges, multilateralism likely reflects the geopolitical challenges, coordination hurdles, and resources required in a large-scale combat operational environment.

Discussion

Almost every nation-state participated in military exercises over the past 30 years.[1] Over 50 percent of bilateral exercises in recent years were between non-allies, while a substantial portion of multilateral exercises included at least one non-allied relationship. This suggests that while bilateral exercises almost certainly (86-99%) will continue, the increase rate for multilateral exercises will likely outpace bilateral. [H]

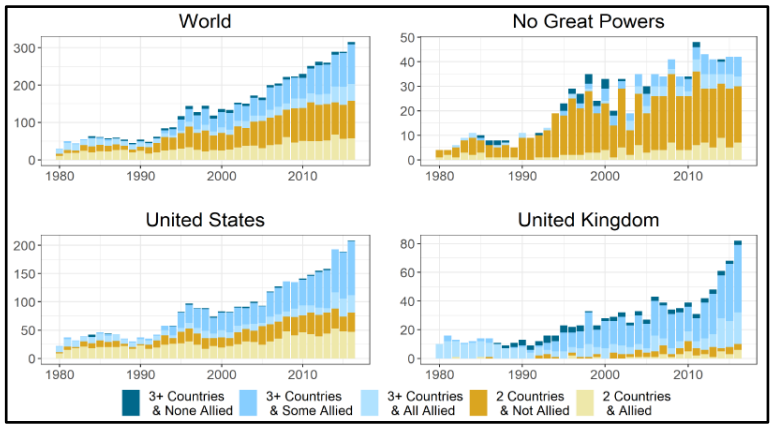
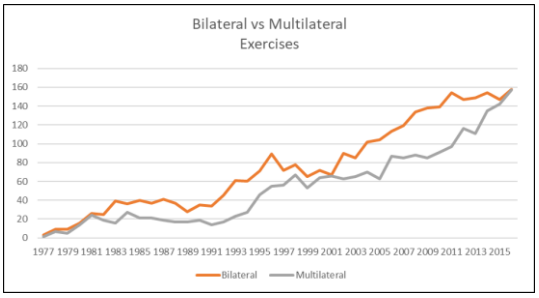


Figure 32 Graph of military exercises since 1980. Harvard

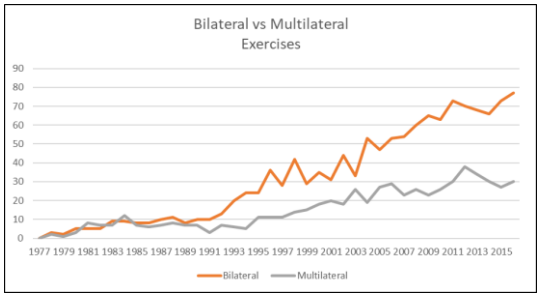
Global security concerns interconnect, requiring coalitions to collaborate and share resources to address health, environmental, criminal, migration, and poverty crises. NATO exercises integrate military and civilian organizations to test capabilities and practices before a crisis. [M] Large-scale military exercises project collective strength, highlight shared interests, and underscore a commitment to collaboration. DEFENDER Europe focuses 14 countries on strategically deploying US-based forces and employing Army Prepositioned Stocks to build readiness between US and NATO forces. [H] MALABAR is a quadrilateral exercise that spanned the Pacific and Indian Oceans, with different phases focusing on special operations, anti-submarine warfare, and surface battles demonstrating strength in multiple domains. [M] Multinational exercises foster enhanced confidence and broader understanding by overcoming interoperability barriers not understood through bilateral engagements. RIMPAC (Rim of the Pacific), a 26-nation

[1] Bernhardt, Jordan, 2021, "Joint Military Exercises Dataset", https://doi.org/10.7910/DVN/HXQFHU, Harvard Dataverse, V1, 42.

maritime exercise, includes unscripted portions, forcing leaders to think through coordination challenges across diverse commands in unknown environments. [H]



United States involved in exercise.



United States not involved in exercise.

Bilateral exercises offer specific advantages that multilateral exercises are unlikely (31-45%) to replicate. Two-country exercises are likely to tailor training and intensity toward a particular objective. Fewer participants require less coordination and logistical support while fostering closer relationships. Only some nations can coordinate multilateral exercises. Finally, bilateral ties are almost sure to have a relevant and vital role in global security. While challenges exist, multilateralism remains essential, reflecting modern conflict's collaborative and resource-sharing aspects, which is crucial for achieving optimal troop ratios in large-scale operations.

Analytic Confidence

This analysis has a *medium* level of confidence. The author carefully evaluated sources using established tools (Trust Scale and Web Site Evaluation Worksheet); however, additional limitations influenced uncertainty. First, the lack of in-depth knowledge of international affairs might lead to misinterpretations or oversimplifications of complex diplomatic implications. Second, instead of conducting solo analysis, collaborative perspectives could strengthen understanding. Third, a structured analytical process, which guides critical source evaluation, was not employed. Finally, economic, cultural, and historical relations introduce inherent unknowns due to potential shifts in power dynamics and technological advancements. To mitigate these limitations, we aided open-source content research with advanced AI platforms like Perplexity and Gemini, which provided valuable information and editorial support.

Author: LTC Michael "Neal" Miller

North Korea Highly Likely to Improve Warhead Delivery Capability by 2027

Executive Summary

North Korea, officially known as the Democratic People's Republic of Korea (DPRK), is highly likely (71-85%) to continue improving its nuclear warhead delivery capability by 2027. This is due to North Korea's inherent need for regime survival, rapid advances in rocket development technology, and the ineffective international response to DPRK's encroachments. Despite perennial Republic of Korea (ROK) and United States' military efforts, rhetoric, and sanctions, the country continues producing, testing, and improving its weapons delivery systems.

Discussion

The DPRK views the West's military presence in the ROK and the region as a direct threat to its regime. [H,H] Due to the growing obsolescence of North Korea's conventional military capabilities, it heavily invests in weapons of mass destruction and asymmetric capabilities. Supreme Leader Kim Jong Un views nuclear weapons and intercontinental ballistic missiles (ICBMs) [H] as the guarantor of his autocratic rule, and he has no intention of abandoning those programs. [H]

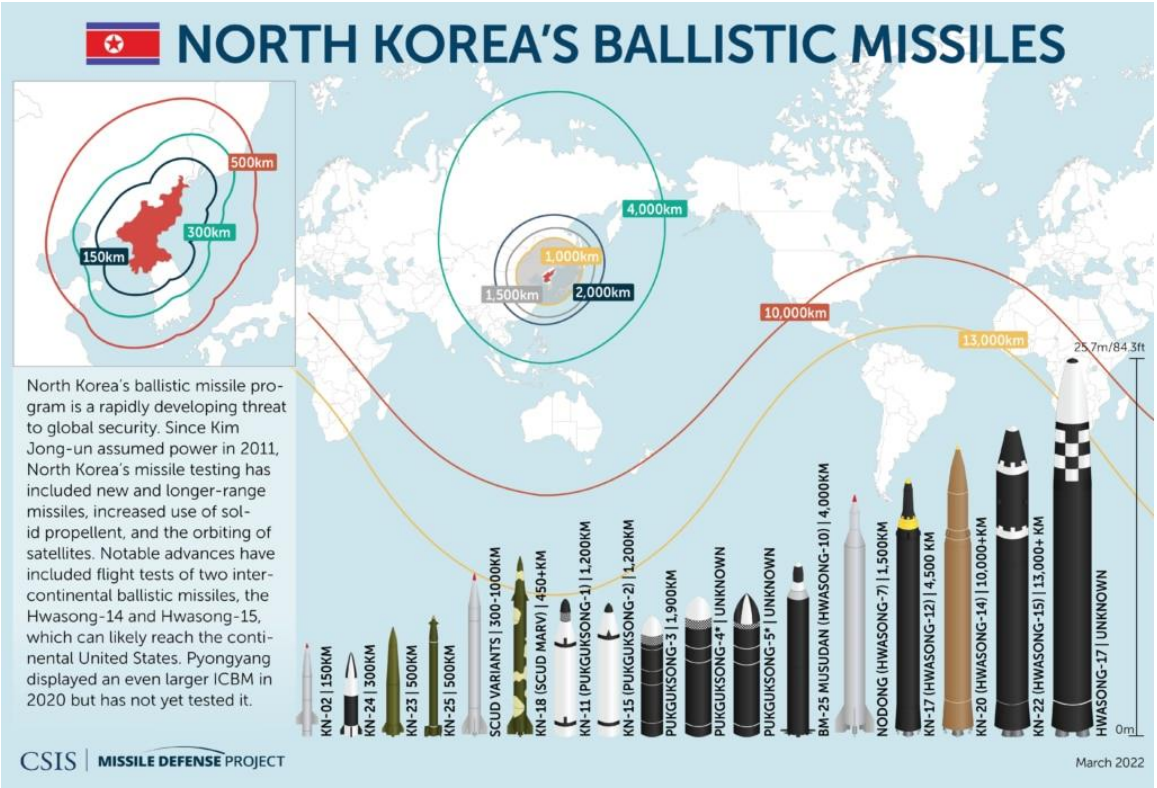


Figure 33 Map Showing Ranges of North Korea's Ballistic Missile CSIS

The country experienced significant advances in its missile technology in the last three decades. Those advances may include testing a new intermediate-range missile tipped with a hypersonic warhead. [H] Solid-fuel intercontinental ballistic missiles, such as the Hwasong-18, target American locations within striking distance of the DPRK. North Korea's ICBM was one of the primary motives for developing and deploying the US Ground-based Midcourse Defense System to protect the American homeland. [H] Recent advances in Supreme Leader Kim Jong Un's ballistic missile testing program could conceivably defeat or degrade the effectiveness of America and allies' systems [Patriot, Aegis Ballistic Missile Defense (BMD), and Terminal High Altitude Area Defense (THAAD).] [H] The DPRK's progress with submarine-launched ballistic missiles (SLBM) suggests an effort to counter land-based THAAD missile defenses. [H] North Korea announced that they designed this SLBM, which is launchable from ballistic missile submarines, for cold launch with solid fuel and it will carry a nuclear warhead. [H]

The overall effectiveness of the international response to the country's weapons testing program is unclear. However, while the international community may have slowed the DPRK's missile program, it is clearly unstoppable. [H,H,H] Supreme Leader Kim Jong Un balks at the international community and recently provided weapons to Russia for use against Ukraine. [H] North Korea's weapons testing program, which began as early as 1989, increased over time. The DPRK, China, the Republic of Korea, the US, and its allies all realize the enormous potential death toll from another armed conflict with the country. While that reasonably stabilizes the ceiling of potential conflict, it does not mean there is space for any conflict. [H] Despite strong Department of State (DoS) statements; joint, combined, and multinational exercises; and United Nations (UN) sanctions, Supreme Leader Kim Jong Un's nuclear weapon delivery capability remains an international concern because the Hermit Kingdom can keep other military forces at bay while threatening the international communities' population centers. [H,H,H,H]

Analytical Confidence

The analytic confidence for this estimate is moderate to *high*. Sources received a high trust score and tended to corroborate one another. However, the analyst worked alone and did not use a structured method. Furthermore, given the volatile, uncertain, complex, and ambiguous (VUCA) operational environment on the Peninsula, this report may change due to new information.

Author: COL John E. Cooper

North Korea Highly Likely to Continue Self-Sustaining Nuclear Program Through 2027 and Beyond

Executive Summary

The Democratic People's Republic of Korea (DPRK) is highly likely (71-85%) to continue its self-sustaining nuclear program through 2027 and beyond. The international community's condemnation and sanctions, aimed at curbing North Korea's nuclear program, have inadvertently fueled its development and financing. Despite the investment of billions of dollars from governments around the globe to keep nuclear material out of the hands of bad actors, the North Korean nuclear program continues to progress.

Discussion

The North Korea regime's interest in nuclear weapons began in the early 1950s out of a sense of self-defense from the West and gained momentum when the former Soviet Union provided vast technical assistance to the country in constructing the Yongbyon Nuclear Research Center in the 1960s. [H] However, the DPRK's nuclear weapons program is now primarily self-sustained. The country's governing leaders maintain the paradigm that nuclear weapons are the ultimate deterrent against the international community. [H] The country consistently acts from its deeply held national values of self-defense and will continue on a nuclear course because there is no other way from its point of view to achieve its national interests.

Type(s) of Nuclear Weapon in a Possible Arsenal	Median	Range of Number of Nuclear Weapons	Constraints
All simple fission weapons	72	55 to 96	Uranium and plutonium stock
All composite-core fission weapons	20	17 to 23	Plutonium stock
Mix of one-stage thermonuclear weapons and simple fission and/or composite-core	49	31 to 74	Uranium and plutonium stock
Combination of three estimates	46	35 to 63	Averaging

Figure 34 North Korea's Nuclear Weapons arsenal. ISIS

The international community's condemnation, military superiority, and economic sanctions triggered North Korea's innovative approach towards gearing its nuclear delivery platforms to match the capabilities of its superior adversaries. One example of this innovation is producing fissile material (plutonium and highly enriched uranium). [H] Another example is the recent tests of the Haeil-5-23, a nuclear-capable underwater attack drone. [H] The chance that the DPRK will diverge from that paradigm is remote. The same international pressures forced North Korea economic resourcefulness and financial

innovation. The country is highly likely not to diverge from a creative approach. [H] Consequently, there are concerns over the country's aggressive nuclear technology and the bad actors who might buy it. [H,H]

However, diplomatic efforts at the highest levels of government, could, by their nature, soften North Korea's position on nuclear weapons. [H] The easing or tightening of sanctions could reasonably influence the DPRK's position. [H] Enhanced security guarantees from the international community could dissuade North Korea from its entrenched position on nuclear weapons. However, it is unknown whether this approach will win the DPRK's support or encourage its aggression. [H] If the international community supported such a program under strict regulations, it could potentially change North Korea's desire to build its nuclear weapons program. A dramatic change in the political climate in the region may also occur if the North Korean government is permitted to maintain its right to a civilian nuclear program, and this includes the production of electricity and medical isotopes, deemed essential by Pyongyang. [H]

Analytical Confidence

The analytic confidence for this estimate is *high*. Sources received very high trust scores and tended to corroborate one another. However, the analyst worked alone and did not use a structured method. This report could change based on diplomatic efforts, sanctions, security guarantees, and the DPRK's civilian nuclear program. Furthermore, given the volatile, uncertain, complex, and ambiguous (VUCA) operational environment on the Peninsula, this report may change due to new information.

Author: COL John E. Cooper

Foreign Support Highly Unlikely to Bolster North Korea's Nuclear Program Through 2027 and Beyond

Executive Summary

Foreign government and private business support is highly unlikely (16-30%) to bolster North Korea's nuclear program through 2027 and beyond due to the country's underdeveloped economic landscape and the restrictive approach its regime takes towards foreign business cooperation. Despite receiving no support from the world's leading nuclear research and development (R&D) companies and limited financial support from Russian and Chinese businesses, the DPRK's nuclear program advances**.** North Korea profits financially from the country's illicit practices such as cybercrime and trafficking in nuclear/other radioactive material.

Discussion

Any support for the Democratic People's Republic of Korea (DPRK) nuclear weapons program is highly unlikely provided by any of the 28 leading private companies involved in the R&D of nuclear weapons technology, their parent nations, or any internationally approved business. [H,H,H] The involvement of those companies in nuclear weapons technology is subject to international laws, regulations, and scrutiny. [H] Therefore, any private companies supporting North Korea would be secretive, illegal, and devoid of the competitive advantages of a capitalistic economy.

Limited financial support **is** highly likely coming from Russian and Chinese businesses. [H,H] The country**'s** authorities generally let the aforementioned private businesses and few others operate, provided they are properly registered and pay taxes. [H,H,H] According to one report, there were more than 215 joint ventures between China and the DPRK and about 30 with Russian joint firms as of the end of September 2023. [H]

Future support could conceivably come from South Korea, whose proposals for inter-Korean economic cooperation included a "New Economic Map" and prioritizing infrastructure projects like railways. [H] Future support could even come from the US Several American companies, such as The Coca-Cola Company, Starbucks Coffee, and McDonald's, signaled interest in business in North Korea but to no avail. [H] It is unlikely that the country will authorize external investment from the US or its allies and their legitimate external private businesses or companies.

The DPRK presently makes money from illicit means. There are reports of illegal or unauthorized activities involving nuclear and other radioactive materials. [H] For example, the International Atomic Energy Agency (IAEA) reported 344 cases of trafficking/malicious use of nuclear/other radioactive material since 1993. [H] The country finances nuclear weapons through an illegal arm smuggling network. [H, H] It is highly likely that the country will continue the weapons-for-money relationship with Russia and continue lead the world in crypto theft.

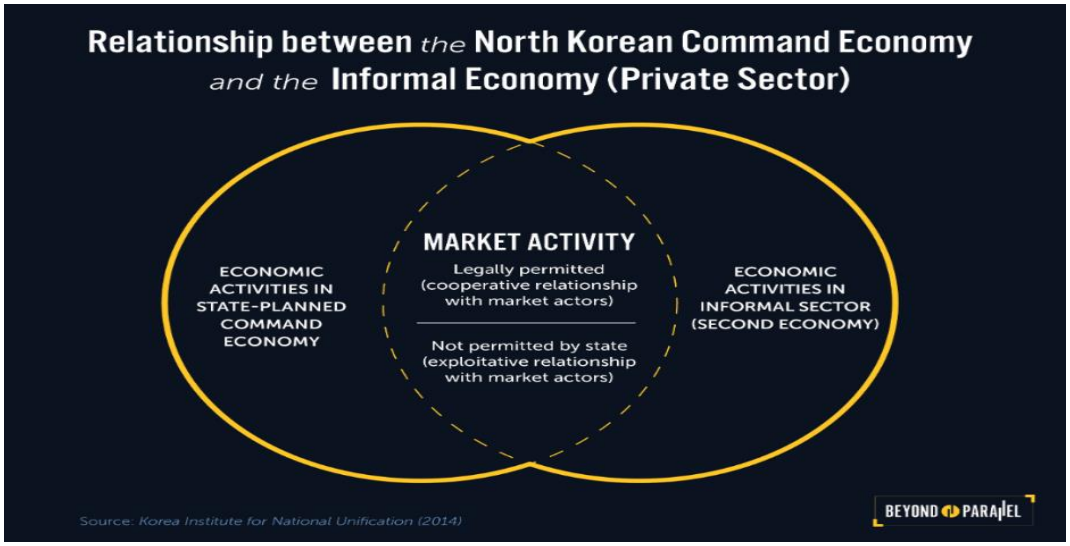


Figure 35 North Korean State vs. Non-State Economy. CSIS

Despite potential opportunities, the country's lack of infrastructure and transparency makes it a risky business environment for both South Korean and US companies. [H] The DPRK's infrastructure requires significant investment to develop its economy. The estimates for such development range from USD 63 billion to 270 trillion for railways, roads, and energy. Compounding its infrastructure challenges are that the country lacks transparency and global standards; statistics are unavailable; labor laws differ significantly from South Korea's; and underground resource estimates are unreliable. [H] Potential value is high, but profitability is questionable due to infrastructure and quality issues. [H]

A large change in capital investments and profits from the international community could hyper-fund the country's nuclear program or change policy by widely introducing ideas such as de-escalation. Those large shifts take time to predict. Reports indicate that the private sector has become a significant economic actor in North Korea, overtaking state-led agents in recent years. The growing influence of the private sector suggests that an increasing number of private companies are involved in business activities with the country. [H,H,H] It is unknown how the DPRK uses the speculated profits.

Analytical Confidence

The analytic confidence for this estimate is *high*. Sources received very high trust scores and tended to corroborate one another. However, the analyst worked alone and did not use a structured method. Furthermore, given the volatile, uncertain, complex, and ambiguous (VUCA) operational environment on the Peninsula, this report may change due to new information. Significant private sector business expansion into the DPRK economy might change this report's forecast.

Annex A – Terms of Reference

Dynamics of Warfare and the Competitive Space 2035

Requirement:
How will innovations[2] from contemporary[3] conflicts likely shape the future dynamics of warfare, and what does it mean for Large Scale Combat Operations (LSCO) and pacing threats by 2035[4]?

- What are likely potential changes to future warfighting functions?
- What are the likely impacts on future regional alliances, partnerships, and relationships?

Methodology:
The team intends to gather information through various means, including but not limited to data collection from open-source outlets and interviews with academia, interest area experts, political scientists, military strategists, and international analysts. Analysts may use multiple formats and remain adaptable to analyze the operational environment and impacts on warfighting functions, regional partnerships, and the overall effect on LSCO.

The team expects to execute this project in the following four steps (Note: This is a notional timeline only. The team will remain flexible to take advantage of opportunities and to address unforeseen limitations that may arise):

Step 1: Data collection (November 2023 – February 2024)

- Identify, analyze, and evaluate contemporary conflicts and their impact on the future operational environment.
- Evaluate the future operational environment's impact on warfighting functions.
- Explore the implications of conflicts and their role in partnerships, alliances, and relationships in shaping the future landscape of power.
- Step 2: Synthesize (February – March 2024)
- Evaluate the research findings.
- Step 3: Compile concepts and prepare a report (March 2024)
- Compile a comprehensive report and conduct peer review with other US Army War College futures seminar class members.
- Step 4: Out-brief Mr. Sullivan and his team (April 2024)

Challenges:
- The team's personnel are executing this study to complete a US Army War College requirement and a full course load for a graduate degree.
- This estimate must be completed by April 2023.

[2] Defined as both material and non-material innovations.
[3] Contemporary conflicts are within the last five years; however, the team will use discretion as needed.
[4] Timeframe begins in 2027 and extends out to 2035.

- Limited funding is available to support travel and other related expenses.
- Due to time and equipment constraints, the team can only access open-source information, and the final product will be unclassified.
- The quantity, character, and context of all contemporary conflicts – and any significant related changes that occur too quickly or unbeknownst to the team – may impact the final product's findings.
- Research on adversaries may require translating languages where no team member is fluent; cultural knowledge is also limited.
- DoD might change its joint warfighting functions, which may not align with this project's analysis or outcomes.

Resources:

- The team utilizes the US Army War College databases and other commercial and educational resources.
- As needed, the team connects with subject matter experts.
- The team utilizes open-source media and published information from academic and professional institutes.
- The team consists of military officers with diverse backgrounds such as: specialties in logistics, human resource and aviation, active duty and reserve Officers.
- Personnel will leverage personal and professional relationships with domestic and international colleagues spanning military, government, academic, organizational, and institutional entities.

Administration:

- The final product will be provided in PDF format and is for the sole use of Ian Sullivan, D/CoS G2 for TRADOC, and anyone he designates.
- The draft out-brief will be ready for presentation upon completion of peer review, with the final out-brief in April 2023.
- The research team includes:
    - Team Point of Contact:
        - LTC John Cooper, (757) 848-6739, john.e.cooper14.mil@armywarcollege.edu
    - Alternate Team Point of Contact:
        - LTC Joseph Bell, (931) 561-4475, joseph.c.bell2.mil@armywarcollege.edu
    - Additional Team Members:
        - LTC Kristine Hinds, (915) 588-3078, kristine.m.hinds.mil@armywarcollege.edu
        - LtCol Erik Keim, (307) 258-9020, erik.a.keim.mil@armywarcollege.edu
        - LTC Michael "Neal" Miller, (859) 227-0555, michael.miller456.mil@armywarcollege.edu
    - Official Email Address: awc24_sullivan@armywarcollege.edu.

Annex B – Trust Scale and Web Site Evaluation Worksheet

The Trust Scale and Web Site Evaluation Worksheet calculates an estimate of how trustworthy sources were in developing a forecast based on the following criteria. The next few pages include topics, articles, and the trust scale value.

Trust Scale and Web Site Evaluation Worksheet									
Piece of Evidence #:			**1**	**2**	**3**	**4**	**18**	**19**	**20**
Criteria	**Tips**	**Value**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**
Content can be corroborated?	Check some of the site's facts	5.17							
Recommended by subject matter expert?	Doctor, biologist, country expert	4.94							
Author is reputable?	Google for opinions, ask others	4.64							
You perceive site as accurate?	Check with other sources; check affiliations	4.56							
Information was reviewed by an editor or peers?	Science journals, newspapers	4.52							
Author is associated with a reputable org?	Google for opinions, ask others.	4.42							
Publisher is reputable?	Google for opinions, ask others.	4.02							
Authors and sources identified?	Trustworthy sources want to be known	3.78							
You perceive site as current?	Last update?	3.78							
Several other Web sites link to this one?	Sites only link to other sites they trust	3.68							
Recommended by a generalist?	Librarian, researcher	3.65							
Recommended by an independent subject guide?	A travel journal may suggest sites	3.56							
Domain includes a trademark name?	Trademark owners protect their marks	3.45							
Site's bias in clear?	Bias is OK if not hidden	3.06							
Site has professional look?	It should look like someone cares	2.86							
	Total:	**60.09**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	Trust Scale:								

19 Dec 2001: The criteria and weighted values are based on a survey input from 66 analysts. For details see: http://daxrnorman.googlepages.com/analysis. Edited for simplicity by Kristan J. Wheaton, OCT 2013
3 Feb 2012: Excel Spreadsheet which adds auto-sum was produced by Bill Welch, Deputy Director, Center for Intelligence Research Analysis and Training, Mercyhurst College.
26 Jan 2013: Trust Scale and Web Site Evaluation Worksheet is in the PUBLIC DOMAIN.

Trust Scale	
Minimum Value	**Credibility**
46.75	Very High
40	High
35.06	Moderate
21	Low
7.46	None

Source Websites		
#	**Credibility**	**Link**
1		
2		
3		
4		
5		
18		
19		
20		

Shifting Alliances and Technological Innovations Likely to Redefine Global Balance of Power by 2035		
##	*Trust Scale*	*Article*
1	*Very High*	**The Revolution in Military Affairs: A Framework for Defense Planning** *https://press.armywarcollege.edu/monographs/265/*
2	*Very High*	**VIDEO: THE THIRD U.S. OFFSET STRATEGY AND ITS IMPLICATIONS FOR PARTNERS AND ALLIES** *https://warontherocks.com/2015/01/video-the-third-u-s-offset-strategy-and-its-implications-for-partners-and-allies/*
3	*Very High*	**RAND U.S. Security-Related Agreements in Force Since 1955; Introducing a New Database** *https://www.rand.org/pubs/research_reports/RR736.html*
4	*Very High*	**Houthis may be running low on their weapons stocks as attacks on ships slow, US commander** *https://apnews.com/article/houthi-attacks-ships-red-sea-7b86941c985a934281c68d6624baff1b*
5	*Very High*	**THE ARMY AND THE FORTRESS FLEET: REIMAGINING LANDPOWER IN MARITIME WARFARE** *https://mwi.westpoint.edu/the-army-and-the-fortress-fleet-reimagining-landpower-in-maritime-warfare/*
6	*Moderate*	**BAE Systems: Global Combat Air Programme** *https://www.baesystems.com/en/product/global-combat-air-programme*
7	*Moderate*	**Deep learning to translate between programming languages programming languages** *https://ai.meta.com/blog/deep-learning-to-translate-between-programming-languages/*
8	*Very High*	**Distributed Ledger Technology for the systematic Investigation and Reduction of Information Asymmetry in Collaborative Networks** *https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/e49a6322-c61d-478f-9f72-af3f5d890573/content*
9	*Moderate*	**Japan Ministry of Defense: Major Exercises in the Indo-Pacific** *https://www.mod.go.jp/en/d_architecture/major-exercises/major_exercises_02.html*
10	*High*	**A model for types and levels of human interaction with automation** *https://ieeexplore.ieee.org/document/844354*
11	*High*	**A FRENCH OPINION ON THE ETHICS OF AUTONOMOUS WEAPONS** *https://warontherocks.com/2021/06/the-french-defense-ethics-committees-opinion-on-autonomous-weapons/*
12	*High*	**RAND - Russia's Asymmetric Response to 21st Centruy Strategic Competition** *https://www.rand.org/pubs/research_reports/RRA1233-5.html*
13	*High*	**United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects** *https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_WP.4_Rev1.pdf*

14	*High*	**China's Strategic Ambiguity on the Issue of Autonomous Weapon Systems**
		https://scholarhub.ui.ac.id/global/vol24/iss1/1/
15	*High*	**United Kingdom's Ambitious, Safe, and Responsible Policy**
		https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082991/20220614-Ambitious_Safe_and_Responsible.pdf
Nations Almost Certainly Will Use Lethal Autonomous Weapons System in Combat by 2035		
##	*Trust Scale*	*Article*
1	*High*	**RAND - Russia's Asymmetric Response to 21st Century Strategic Competition**
		https://www.rand.org/pubs/research_reports/RRA1233-5.html
2	*High*	**United States Department of Defense Directive 3000.09, Autonomy in Weapon Systems**
		https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf
3	*High*	**China's Strategic Ambiguity on the Issue of Autonomous Weapon Systems**
		https://scholarhub.ui.ac.id/global/vol24/iss1/1/
4	*High*	**United Kingdom's Ambitious, Safe, and Responsible Policy**
		https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082991/20220614-Ambitious_Safe_and_Responsible.pdf
5	*High*	**A model for types and levels of human interaction with automation**
		https://ieeexplore.ieee.org/document/844354
6	*High*	**Human Rights Watch: Losing Humanity - The Case against Killer Robots**
		https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots
7	*High*	**United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects**
		https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_WP.4_Rev1.pdf
8	*Very High*	**Automated Decision Research: State Positions on Negotiating Legally Binding Instruments on AWS**
		https://automatedresearch.org/state-positions/
9	*Very High*	**Military Strategy Magazine: Drones in the Nagorno-Karabakh War - Analyzing the Data**
		https://www.militarystrategymagazine.com/article/drones-in-the-nagorno-karabakh-war-analyzing-the-data/
10	*High*	**NPR: A Military Drone With A Mind Of Its Own Was Used IN Combat, U.N. Says**
		https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d
11	*High*	**Insight Turkey: The Role of Turkish Drones in Azerbaijan's Increasing Military Effectiveness: An Assessment of the Second Nagorno-Karabakh War**

		https://www.insightturkey.com/articles/the-role-of-turkish-drones-in-azerbaijans-increasing-military-effectiveness-an-assessment-of-the-second-nagorno-karabakh-war
12	*High*	**Arms Control Association: Autonomous Weapons Systems and the Laws of War**
		https://www.armscontrol.org/act/2019-03/features/autonomous-weapons-systems-laws-war
13	*High*	**A FRENCH OPINION ON THE ETHICS OF AUTONOMOUS WEAPONS**
		https://warontherocks.com/2021/06/the-french-defense-ethics-committees-opinion-on-autonomous-weapons/
Quantum Computing Highly Likely to Revolutionize Military Logistics Before 2035		
##	*Trust Scale*	*Article*
1	*Moderate*	**Honeywell: How BMW Can Maximize Its Supply Chain Efficiency With Quantum**
		https://www.honeywell.com/us/en/news/2021/01/exploring-supply-chain-solutions-with-quantum-computing
2	*Very High*	**IEEE: Quantum Computing for Dummies**
		https://spectrum.ieee.org/quantum-computing-for-dummies
3	*High*	**Forbes: Quantum Computing Expanded in 2021, Setting Up A Big 2022**
		https://www.forbes.com/sites/danielnewman/2022/01/10/quantum-computing-expanded-in-2021-setting-up-a-big-2022/?sh=521cc02581b8
4	*Very High*	**Modern War Institute: Logistics Determine Your Destiny: What Russia's Invasion is (Reteaching Us About Contested Logistics**
		https://mwi.usma.edu/logistics-determine-your-destiny-what-russias-invasion-is-reteaching-us-about-contested-logistics/
5	*High*	**Forbes: 13 Risks That Come With The Growing Power of Quantum Computing**
		https://www.forbes.com/sites/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/
6	*Moderate*	**Congressional Website: Reps. Obernolte, Stevens introduce new bill to accelerate quantum computing applications in US**
		https://obernolte.house.gov/media/press-releases/reps-obernolte-stevens-introduce-new-bill-accelerate-quantum-computing
7	*Very High*	**National Science Foundation invests $38 million in quantum research**
		https://fedscoop.com/nsf-invests-38-million-in-quantum-research/
8	*Very High*	**Department of Energy Announces $11.7 Million for Research on Quantum Computing**
		https://www.energy.gov/science/articles/department-energy-announces-117-million-research-quantum-computing
Machine Learning Likely to Boost Interoperability in US-Allied Defense Strategy Before 2030		
##	*Trust Scale*	*Article*
1	*Very High*	**CSIS: Battle Networks and the Future Force, Part 3**
		https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220304_Harrison_Battle_Networks_3.pdf
2	*Very High*	**Speech and Language Processing: Machine Translation, Chapter 13**
		https://web.stanford.edu/~jurafsky/slpdraft/13.pdf
3	*Very High*	**CBO: The U.S. Military's Force Structure: A Primer, 2021 Update**
		https://www.cbo.gov/publication/57088

4	*Very High*	**CSBA: Toward a New Offset Strategy - Exploiting US Long-Term Advantages to Restore US Global Power Projection Capability**
		https://csbaonline.org/uploads/documents/Offset-Strategy-Web.pdf
5	*Very High*	**SIPRI: Top 100 arms-producing and military services companies in the world, 2022**
		https://www.sipri.org/visualizations/2023/sipri-top-100-arms-producing-and-military-services-companies-world-2022
6	*Low*	**Localize: The Ultimate Guide to Real-Time Language Translation**
		https://localizejs.com/articles/everything-you-want-to-know-about-real-time-translation/
7	*Very High*	**RAND: Lessons Learned from the Afghan Mission Network - Developing a Coalition Contingency Network**
		https://www.rand.org/pubs/research_reports/RR302.html
8	*Very High*	**NATO: Partnership Interoperability Initiative**
		https://www.nato.int/cps/en/natohq/topics_132726.htm
9	*Moderate*	**Deep learning to translate between programming languages programming languages**
		https://ai.meta.com/blog/deep-learning-to-translate-between-programming-languages/
Multilateral Exercises Likely to Outpace Bilateral Exercises Before 2035		
##	*Trust Scale*	*Article*
1	*Very High*	**Joint Military Exercises Dataset (30 Years)**
		https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/HXQFHU
2	*Very High*	**The Causes and Consequences of Joint Military Exercises**
		https://stacks.stanford.edu/file/druid:kb768wv0832/BernhardtJordanDissertation-augmented.pdf
3	*Moderate*	**NATO Exercises**
		https://www.nato.int/cps/en/natohq/topics_49285.htm
4	*Moderate*	**Japan Ministry of Defense: Major Exercises in the Indo-Pacific**
		https://www.mod.go.jp/en/d_architecture/major-exercises/major_exercises_02.html
5	*Very High*	**USNI: RIMPAC 2022 Officials Reflect on Lessons Learned, What to Change for RIMPAC 2024**
		https://news.usni.org/2022/08/04/rimpac-2022-officials-reflect-on-lessons-learned-what-to-change-for-rimpac-2024
6	*Very High*	**CSIS: Battle Networks and the Future Force, Part 3**
		https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220304_Harrison_Battle_Networks_3.pdf
7	*High*	**U.S. Army Europe and Africa Exercises**
		https://www.europeafrica.army.mil/Exercises/
Virtual Deception Will Almost Certainly Drive a Shift in Intelligence-Sharing Strategies by 2030		
##	*Trust Scale*	*Article*
1	*Very High*	**RAND: Lessons Learned from the Afghan Mission Network - Developing a Coalition Contingency Network**
		https://www.rand.org/pubs/research_reports/RR302.html
2	*Very High*	**CSIS: Battle Networks and the Future Force, Part 3**
		https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220304_Harrison_Battle_Networks_3.pdf

3	*Very High*	**RAND: Prioritizing Security Cooperation with Highly Capable U.S. Allies - Framing Army-to-Army Partnerships**
		https://www.rand.org/pubs/research_reports/RRA641-1.html
4	*Very High*	**USAWC: A Call to Action: Lessons from Ukraine for the Future Force**
		https://press.armywarcollege.edu/parameters/vol53/iss3/4/
5	*Very High*	**ODNI: National Intelligence Strategy 2023**
		https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf
6	*Very High*	**Atlantic Council: In brief - A ten-step guide to transforming intelligence sharing with US allies**
		https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/in-brief-a-ten-step-guide-to-transforming-intelligence-sharing-with-us-allies/
7	*Moderate*	**archTIS: Securing Multinational Coalition Collaboration with Data-Centric Security**
		https://www.archtis.com/securing-multinational-coalition-collaboration-with-data-centric-security/
8	*Very High*	**Distributed Ledger Technology (Incl. Blockchain) Use Cases - Digital Assets, AI, and Beyond**
		https://www.jdsupra.com/legalnews/distributed-ledger-technology-incl-8567075/
9	*Very High*	**Distributed Ledger Technology for the systematic Investigation and Reduction of Information Asymmetry in Collaborative Networks**
		https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/e49a6322-c61d-478f-9f72-af3f5d890573/content
10	*High*	**Contextualizing Deepfake Threats to Organizations**
		https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF
11	*Moderate*	**9 Smart contract vulnerabilities and how to mitigate them**
		https://www.techtarget.com/searchsecurity/tip/Smart-contract-vulnerabilities-and-how-to-mitigate-them
12	*Very High*	**New US Intelligence Strategy Calls for More Partners, More Sharing**
		https://www.voanews.com/a/new-us-intelligence-strategy-calls-for-more-partners-more-sharing-/7220725.html
Use of Autonomous Semi-Submersibles for Logistics Resupply Missions Likely by 2035		
##	*Trust Scale*	*Article*
1	*Very High*	**Narco-Subs: A Game of Hide-and-Seek**
		https://www.afcea.org/signal-media/technology/narco-subs-game-hide-and-seek
2	*Very High*	**A Secret Shipyard Building Submarines for Drug Cartels Just Got Busted**
		https://www.vice.com/en/article/epvdgz/colombia-narco-sub-shipyard-bust
3	*Very High*	**US Navy's four unmanned ships return from Pacific deployment**
		https://www.defensenews.com/naval/2024/01/16/us-navys-four-unmanned-ships-return-from-pacific-deployment/
4	*Very High*	**For survivable resupply, look to autonomous submarines**

		https://www.c4isrnet.com/opinion/2023/11/08/for-survivable-resupply-look-to-autonomous-submarines/
5	*Very High*	**Attention Turns to Extra Large Unmanned Underwater Vessels** https://www.marinelink.com/news/attention-turns-extra-large-unmanned-498317
Space-to-Cellphone Likely by 2030: Revolutionizing Military Communications		
##	*Trust Scale*	*Article*
1	*Very High*	**Elon Musk's Starlink Launches First-Ever Cell Service Satellites—Here's What To Know And What Mobile Phone Carrier Gets It First** https://www.forbes.com/sites/roberthart/2024/01/03/elon-musks-starlink-launches-first-ever-cell-service-satellites-heres-what-to-know-and-what-mobile-phone-carrier-gets-it-first/
2	*High*	**Starlink Successfully Tests Space Direct to Cell Mobile Service** https://www.ispreview.co.uk/index.php/2024/01/starlink-successfully-tests-space-direct-to-cell-mobile-service.html
3	*High*	**China could launch 13,000 satellites to "suppress" and spy on Starlink** https://www.techspot.com/news/97721-china-could-launch-13000-satellites-suppress-spy-starlink.html
Blending in the Electromagnetic Spectrum Highly Likely to Decrease Probability of Detection and Interception of Communications by 2030		
##	*Trust Scale*	*Article*
1	*Very High*	**Ukraine Uses Off-The-Shelf Electronics To Target Russian Communications** https://www.forbes.com/sites/davidhambling/2022/11/03/ukraine-uses-off-the-shelf-electronics-to-target-russian-communications/?sh=224f3df45fc81
2	*Very High*	**How Ukrainian DIY Drones Are Taking Out Russian Tanks** https://www.wsj.com/video/series/in-depth-features/how-ukrainian-diy-drones-are-taking-out-russian-tanks/3912093C-EDC6-4EDE-806D-57C558C8E8DB
3	*Very High*	**Hiding in plain sight: Warfare in the electromagnetic spectrum** https://www.c4isrnet.com/opinion/2023/08/01/hiding-in-plain-sight-warfare-in-the-electromagnetic-spectrum/
4	*Very High*	**Modern Electromagnetic Spectrum Battlefield** https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846737/modern-electromagnetic-spectrum-battlefield/
5	*High*	**What We've Learned About SDRs From Russia's War On Ukraine** https://www.rfglobalnet.com/doc/what-we-ve-learned-about-sdrs-from-russia-s-war-on-ukraine-0001
Use of Networked Acoustic Sensors for Integrated Air Defense Almost Certain by 2035		
##	*Trust Scale*	*Article*
1	*Very High*	**Ukraine Using Thousands Of Networked Microphones To Track Russian Drones** https://www.twz.com/land/thousands-of-networked-microphones-are-tracking-drones-in-ukraine
2	*Very High*	**Gunshot Airborne Surveillance with Rotary Wing UAV-Embedded Microphone Array** https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6806267/
3	*Very High*	**Acoustic Mortar Localization System - Results from OIF** https://apps.dtic.mil/sti/citations/ADA431658
4	*Very High*	**Leidos is building advanced air defense sensors for the Marines**

		https://cummingsresearchpark.com/2023/06/22/leidos-is-building-advanced-air-defense-sensors-for-the-marines/
5	*High*	**Patria MUSCL passive radar system**
		https://www.youtube.com/watch?v=36N_6mC_qrc
Free Space Optics Highly Likely to Ensure Reliable, Secure Communications in Future Conflicts by 2035		
##	*Trust Scale*	*Article*
1	*Very High*	**Global communications are under attack — optical satellite networks can bolster them**
		https://spacenews.com/global-communications-under-attack-optical-satellite-networks-bolster/
2	*Very High*	**Okinawa Marines Test Future of Wireless Communications**
		https://www.defense.gov/News/News-Stories/Article/Article/1611671/okinawa-marines-test-future-of-wireless-communications/
3	*Very High*	**3 Red Sea data cables cut as Houthis launch more attacks in the vital waterway**
		https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a
4	*Very High*	**Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks**
		https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks
5	*Moderate*	**Free Space Optics (FSO) Communication Market**
		https://www.transparencymarketresearch.com/free-space-optics-market.html
Private Sector Involvement in Future Conflicts Highly Likely to Increase Success by 2027		
##	*Trust Scale*	*Article*
1	*Very High*	**Evaluating the International Support to Ukrainian Cyber Defense**
		https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322
2	*High*	**Recapping "Cyber in War: Lessons From the Russia - Ukraine Conflict"**
		https://lieber.westpoint.edu/recapping-cyber-war-lessons-russia-ukraine-conflict/
3	*High*	**How Ukraine and U.S. Tech Firms Build for the Future**
		https://share.america.gov/how-ukraine-us-tech-firms-build-for-future/
4	*High*	**Occupational Outlook Handbook: Information Security Analysts**
		https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
5	*High*	**Comparison of Public and Private Sector Cybersecurity and IT Forces**
		https://www.rand.org/pubs/research_reports/RRA660-7.html
6	*High*	**North Atlantic Treaty Organization 2030 Fact Sheet**
		https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf
7	*High*	**The Sixth Domain: The Role in the Private Sector in Warfare**
		https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/
8	*High*	**Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack**
		https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html
Rapid War-Time Innovation Required to Compete and Win in 2030 and Beyond		
##	*Trust Scale*	*Article*

1	*High*	**Ukrainian Innovation in a War of Attrition**
		https://www.csis.org/analysis/ukrainian-innovation-war-attrition
2	*High*	**Ukraine Weaponized Pickups - Tiny Grad on the Go**
		https://www.technology.org/2023/04/17/ukraine-weaponized-pickups-tiny-grad-on-the-go/
3	*Medium*	**How a Fleet of Aging Farm Pickup Trucks from Britain is Fooling Russian Snipers**
		https://www.businessinsider.com/russian-snipers-fooled-british-pickup-trucks-ukraine-2022-12
4	*High*	**Enemy Drone that Killed US Troops in Jordan was Mistaken for a US Drone, Preliminary Report Suggests**
		https://apnews.com/article/jordan-drone-attack-attack-confusion-f175962e058b9b6f668303faf248d8e6
5	*High*	**Strategic Trends Programme Future Operating Environment 2035**
		https://assets.publishing.service.gov.uk/media/6286575de90e071f69f22600/FOE.pdf
6	*High*	**Myths and Principles in the Challenges of Future War**
		https://www.ausa.org/publications/myths-and-principles-challenges-future-war
7	*High*	**An Innovative Strategy for the Decisive Decade**
		https://innovation.defense.gov/Portals/63/DIB_An%20Innovation%20Strategy%20for%20the%20Decisive%20Decade_230717_1.pdf
8	*High*	**The Weapons Industry has a 'Need for Speed' but can be Accident Prone**
		https://responsiblestatecraft.org/2023/08/30/breaking-down-the-military-innovation-blame-game/
Ethical and Legal Dilemmas Likely to Impact Lethal Autonomous Weapon System Usage in 2030 and Beyond		
##	*Trust Scale*	*Article*
1	*High*	**Human Machine Teamwork: The Future of Military Collaboration**
		https://www.karveinternational.com/insights/human-machine-teamwork-the-future-of-military-collaboration
2	*High*	**Autonomous Weapon Systems**
		https://link.springer.com/article/10.1007/s10676-018-9494-0
3	*High*	**Autonomous Weapons are the Moral Choice**
		https://www.atlanticcouncil.org/blogs/new-atlanticist/autonomous-weapons-are-the-moral-choice/
4	*Very High*	**Lethal Autonomous Weapon Systems and Respect for Human Dignity**
		https://pubmed.ncbi.nlm.nih.gov/36156937/
5	*Very High*	**Laws on LAWS: Regulating the Lethal Autonomous Weapon Systems**
		https://www.airuniversity.af.edu/JIPA/Display/Article/3533453/laws-on-laws-regulating-the-lethal-autonomous-weapon-systems/
6	*High*	**Stopping Killer Robots**
		https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and
7	*High*	**What you Need to Know about Autonomous Weapons**
		https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons
8	*High*	**Defense Primer: U.S. Policy on Lethal Autonomous Weapons**
		https://crsreports.congress.gov/product/pdf/IF/IF11150

9	*High*	**Russia's Perspective on Human Control and Autonomous Weapons: Is the Official Discourse Changing?**
		https://www.autonorms.eu/russias-perspective-on-human-control-and-autonomous-weapons-is-the-official-discourse-changing-2/
10	*Very High*	**Russia has Probably Not Used AI-Enabled Weapons in Ukraine, but That Could Change**
		https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change
11	*High*	**Weaponized Artificial Intelligence and Chinese Practices of Human-Machine Interaction**
		https://academic.oup.com/cjip/article/16/1/106/6976053?login=false
12	*High*	**"AI Weapons" in China's Military Innovation**
		https://www.brookings.edu/articles/ai-weapons-in-chinas-military-innovation/
Cyber Attacks on Industrial Critical Infrastructure Highly Likely to Impact Military Mobilizations by 2035		
##	*Trust Scale*	*Article*
1	*Very High*	**PRC State Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure**
		https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
2	*High*	**High Impact Attacks on Critical Infrastructure Climb 140%**
		https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/
3	*High*	**80+ Amazing IoT Statistics (2024-2030)**
		https://explodingtopics.com/blog/iot-stats
4	*High*	**Incentives are Key to Breaking the Cycle of Cyberattacks on Critical Infrastructure**
		https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html
5	*High*	**China is Targeting US Infrastructure and Could Wreak "CHAOS" FBI Says**
		https://www.nytimes.com/2024/01/31/us/politics/fbi-director-china-wray-.html
6	*High*	**Opening Statement by CISA Director Jen Easerly**
		https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly
7	*Very High*	**Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario**
		https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario
8	*High*	**Cyber Attack Force a Shutdown of a Top U.S. Pipeline**
		https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
9	*High*	**Terrifying Hacks on Critical Infrastructure Have Arrived, America Isn't Ready**
		https://thehill.com/opinion/cybersecurity/4353922-terrifying-hacks-on-critical-infrastructure-have-arrived-america-isnt-ready/
10	*High*	**Ransomware Attack Hit San Francisco Train System**
		https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/

11	*High*	**Cyber Attack on New York Dam Highlights the Dark Side of the Internet of Things**
		https://observer.com/2016/03/cyber-attack-on-new-york-dam-highlights-the-dark-side-of-the-internet-of-things/
12	*High*	**Analysis of Top 11 Cyber Attacks on Critical Infrastructure**
		https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
13	*High*	**Breaches by Iran-Affiliated Hackers**
		https://www.cbsnews.com/pittsburgh/news/breaches-by-iran-affiliated-hackers-spanned-multiple-u-s-states-federal-agencies-say/
14	*High*	**FBI Director: Chinese Hackers are Targeting US Infrastructure**
		https://www.rfa.org/english/news/china/hackers-civilian-infrastructure-01312024152506.html
15	*Very High*	**Summary 2023 Cyber Strategy of the Department of Defense**
		https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF
17	*High*	**New Intelligence Report Warns China has been U.S. Critical Infrastructure for "At Least Five Years."**
		https://www.msn.com/en-us/news/world/new-intelligence-report-warns-china-has-been-in-us-critical-infrastructure-for-at-least-five-years/ar-BB1hW9Av
18	*High*	**CISA, FBI Warn of China-Linked Hackers Pre-Positioning for Destructive Cyberattacks against US Critical Infrastructure**
		https://therecord.media/cisa-fbi-warn-of-china-linked-hackers-targeting-critical-us-infrastructure
19	*High*	**Explainer: What is Volt Typhoon and Why is it the Defining Threat of our Generation?'**
		https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer
Near Even Chances that the United States Defense Industrial Base is Prepared for Large Scale Combat Operations by 2030		
##	*Trust Scale*	*Article*
1	*High*	**The U.S. Has a Defense Supply Chain Problem**
		https://www.bloomberg.com/news/articles/2023-12-07/arming-israel-ukraine-exposes-a-us-defense-supply-chain-problem
2	*High*	**U.S. Not Ready to Quickly Produce and Ship Weapon Systems Panel Says**
		https://news.usni.org/2023/04/10/u-s-not-ready-to-quickly-produce-and-ship-weapon-systems-panel-says
3	*High*	**How Russia-Ukraine War is Boosting US Economy, Defense Industry**
		https://timesofindia.indiatimes.com/world/us/how-russia-ukraine-war-is-boosting-us-economy-defense-industry/articleshow/107816099.cms
4	*Very High*	**The U.S. Defense Industrial Base is Not Prepared for a Possible Conflict with China**
		https://features.csis.org/preparing-the-US-industrial-base-to-deter-conflict-with-China/
5	*High*	**Ukraine is Bolstering its Defense Industry to Cut Need for Foreign Aid**
		https://www.forbes.com/sites/vikrammittal/2024/01/16/ukraine-is-bolstering-its-defense-industry-to-cut-need-for-foreign-aid/?sh=45807cdb4255
6	*Moderate*	**From Blockchain to COTS, Commercial Teach in Ukraine Is Determining the Future of Modern Warfare**

		https://www.linkedin.com/pulse/from-blockchain-cots-commercial-tech-ukraine-future-modern-mckay
7	*Very High*	**Built in China: Beijing's Defense Industrial Base and Implications for the United States**
		https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-01/NEW_240125_GlobalForecast_2024_ChinaChallenge_Jones.pdf?VersionId=s5H2obT7SDu3n_AaTThxW99cRQ8w5XrC
8	*High*	**Briefer: National Defense Industrial Base**
		https://dsm.forecastinternational.com/2024/01/26/briefer-national-defense-industrial-strategy/
Future Military Success Highly Likely to be Reliant Upon Non-Military Forces by 2030		
##	*Trust Scale*	*Article*
1	*Very High*	**The Sixth Domain: The Role of the Private Sector in Warfare**
		https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/
2	*Very High*	**Supporting Ukraine's Private Sector During Wartime**
		https://www.csis.org/analysis/supporting-ukraines-private-sector-during-wartime
3	*High*	**Ukraine's Cyber Defense Insights Pricate**
		https://www.globsec.org/what-we-do/publications/ukraines-cyber-defence-insights-private-sector-contributions-russian
4	*Very High*	**NATO 2030**
		https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf
5	*High*	**U.S. Not Ready to Quickly Produce and Ship Weapon Systems, Panel Says**
		https://news.usni.org/2023/04/10/u-s-not-ready-to-quickly-produce-and-ship-weapon-systems-panel-says
6	*High*	**The US Has a Defense Supply Chain Problem**
		https://www.bloomberg.com/news/articles/2023-12-07/arming-israel-ukraine-exposes-a-us-defense-supply-chain-problem
7	*High*	**The U.S. Defense Industrial Base Is Not Prepared for a Possible Conflict with China**
		https://features.csis.org/preparing-the-US-industrial-base-to-deter-conflict-with-China/
8	*High*	**Terrifying hacks on critical infrastructure have arrived. America isn't ready.**
		https://thehill.com/opinion/cybersecurity/4353922-terrifying-hacks-on-critical-infrastructure-have-arrived-america-isnt-ready/
9	*High*	**High-impact attacks on critical infrastructure climb 140%**
		https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/
10	*High*	**Summary 2023 Cyber Strategy of the Department of Defense**
		https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF
11	*High*	**FBI director: Chinese hackers targeting US infrastructure**
		https://www.rfa.org/english/news/china/hackers-civilian-infrastructure-01312024152506.html
12	*High*	**How Much U.S. Farmland Does China Really Own? More Than Bill Gates—**

		https://www.forbes.com/sites/emilywashburn/2023/03/01/how-much-us-farmland-does-china-really-own-more-than-bill-gates-and-less-than-17-other-countries/?sh=23d318a1421f
13	*High*	**What Business Needs to Know About the New U.S. Cybersecurity Strategy**
		https://hbr.org/2023/04/what-business-needs-to-know-about-the-new-u-s-cybersecurity-strategy
14	*Very High*	**GSA Industry Partner Message**
		https://www.gsa.gov/system/files/AA%20FASCSA%20Orders%20-%20Message%20Sent%20to%20GSA%20Industry%20Partners.pdf
15	*High*	**Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack**
		https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html
Drone Swarm Advancements Likely to Disrupt Enemy Forces By 2035		
##	*Trust Scale*	*Article*
1	*High*	**The West Must Wake Up to the Iranian Drone Threat**
		https://nationalinterest.org/blog/west-must-wake-iranian-drone-threat-206396
2	*High*	**Drone Swarms: The Good, The Bad, and The Terrifying Future**
		http://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/september/drone-swarms-good-bad-and-terrifying/
3	*High*	**Drones in Ukraine and beyond: Everything you need to know**
		https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/
4	*High*	**MILITARY DRONE SWARM INTELLIGENCE EXPLAINED**
		https://sdi.ai/blog/military-drone-swarm-intelligence-explained/
5	*High*	**Drones in the Nagorno-Karabakh War: Analyzing the Data**
		https://www.militarystrategymagazine.com/article/drones-in-the-nagorno-karabakh-war-analyzing-the-data/
6	*High*	**The Rise of Swarm Drones: A Look at the Latest Advancements in UAV Technology**
		https://www.kdcresource.com/insights-events/the-rise-of-swarm-drones-a-look-at-the-latest-advancements-in-uav-technology/
Foreign Investment in Land and Infrastructure Likely to Increase Vulnerabilities to National Security By 2035		
##	*Trust Scale*	*Article*
1	*High*	**How Much U.S. Farmland Does China Really Own? More Than Bill Gates—And Less Than 17 Other Countries**
		https://www.forbes.com/sites/emilywashburn/2023/03/01/how-much-us-farmland-does-china-really-own-more-than-bill-gates-and-less-than-17-other-countries/
2	*High*	**What Happens When Foreign Investment Becomes a Security Risk?**
		https://www.cfr.org/backgrounder/what-happens-when-foreign-investment-becomes-security-risk
3	*High*	**Foreign ownership of farmland probed at U.S. Senate hearing**
		https://missouriindependent.com/2023/09/28/foreign-ownership-of-u-s-farmland-probed-at-u-s-senate-hearing/
4	*High*	**Foreign Investment in U.S. Agricultural Land Is Raising National Security Concerns**

		https://www.gao.gov/blog/foreign-investment-u.s.-agricultural-land-raising-national-security-concerns#:~:text=Some%20foreign%20investments%20in%20U.S.,Air%20Force%20Base%20in%202022.
5	*High*	**Acquisition- and ownership-related policies to safeguard essential security interests**
		https://www.oecd.org/investment/OECD-Acquisition-ownership-policies-security-May2020.pdf
6	*High*	**Is 'Made in China 2025' a Threat to Global Trade?**
		https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
7	*High*	**Texas drove out Chinese firm, not the wind farm it planned**
		https://apnews.com/article/texas-chinese-wind-farm-green-energy-6cd629303e8870e1942c170ebc52d7bc
US Cyber Defenses and Policies Unlikely to Secure Vulnerabilities By 2035		
##	*Trust Scale*	*Article*
1	*High*	**What Business Needs to Know About the New U.S. Cybersecurity Strategy**
		https://hbr.org/2023/04/what-business-needs-to-know-about-the-new-u-s-cybersecurity-strategy
2	*High*	**A Shared Responsibility: Public-Private Cooperation for Cybersecurity**
		https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity
3	*High*	**GSA Industry Partner Message**
		https://www.gsa.gov/system/files/AA%20FASCSA%20Orders%20-%20Message%20Sent%20to%20GSA%20Industry%20Partners.pdf
4	*High*	**FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy**
		https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
5	*High*	**When humans are the weak link in critical infrastructure cybersecurity**
		https://www.securitymagazine.com/articles/99867-when-humans-are-the-weak-link-in-critical-infrastructure-cybersecurity
6	*High*	**Y2Q Will Be Here Sooner Than You Think**
		https://cybersecurityventures.com/y2q-will-be-here-sooner-than-you-think/
Fortress Fleet Tactic Usage Highly Likely by 2035		
##	*Trust Scale*	*Article*
1	*High*	**Anti-Access and the 'Fortress-Fleet'**
		https://thediplomat.com/2012/09/anti-access-and-the-fortress-fleet/
2	*High*	**Ukraine war: Dramatic images appear to show sinking Russian warship Moskva**
		https://www.bbc.com/news/world-europe-61141118
3	*High*	**THE ARMY AND THE FORTRESS FLEET: REIMAGINING LANDPOWER IN MARITIME WARFARE**
		https://mwi.westpoint.edu/the-army-and-the-fortress-fleet-reimagining-landpower-in-maritime-warfare/
4	*High*	**Naval Fortresses: An Old Concept for a New Era?**
		https://thediplomat.com/2014/08/naval-fortresses-an-old-concept-for-a-new-era/
5	*High*	**An Introduction to the Study of Naval Tactics**

		https://www.usni.org/magazines/proceedings/1900/june/introduction-study-naval-tactics
Weaponized Water in Contemporary Conflict		
##	*Trust Scale*	*Article*
1	*High*	**Water – a weapon of war or a tool for peace?**
		https://siwi.org/latest/water-a-weapon-of-war-or-a-tool-for-peace/
2	*High*	**Water Weaponization: Its Forms, Its Use in the Russia-Ukraine War, and What to Do About It**
		https://climateandsecurity.org/2023/06/water-weaponization-its-forms-its-use-in-the-russia-ukraine-war-and-what-to-do-about-it/
3	*High*	**How Israel's flooding of Gaza's tunnels will impact freshwater supply**
		https://www.aljazeera.com/features/2024/2/3/israel-floods-tunnels-with-seawater-what-impacts-on-gazas-water-supply#:~:text=Israel%20confirmed%20this%20week%20that,in%20the%20besieged%20Palestinian%20enclave.
4	*High*	**Across Africa, water conflict threatens security, health and the environment**
		https://www.downtoearth.org.in/blog/africa/across-africa-water-conflict-threatens-security-health-and-the-environment-86116
5	*High*	**The Situation is Poised to Worsen**
		https://www.wri.org/insights/highest-water-stressed-countries#:~:text=By%202050%2C%20an%20additional%201,by%202100%2C%20an%20optimistic%20scenario.
6	*High*	**Re-Introducing Water to the Armenia-Azerbaijan Agenda: Prospects for Transboundary Water Cooperation in the Post-2020 Peace Processes**
		https://caucasusedition.net/re-introducing-water-to-the-armenia-azerbaijan-agenda-prospects-for-transboundary-water-cooperation-in-the-post-2020-peace-processes/
7	*High*	**Russians are using age-old military tactic of flooding to combat Ukraine's counteroffensive**
		https://theconversation.com/russians-are-using-age-old-military-tactic-of-flooding-to-combat-ukraines-counteroffensive-207589
8	*High*	**Taiwan faces tough water choices**
		https://www.theguardian.com/sustainable-business/taiwan-tough-water-choices
9	*Very High*	**Water and warfare: the battle to control a precious resource**
		https://www.nature.com/articles/d41586-023-03883-w
10	*High*	**Taiwan faces water wake-up call as climate change intensifies**
		https://www.aljazeera.com/news/2021/8/20/taiwan-water-woes
11	*Very High*	**Pacific Institute: Water Conflict Chronology**
		https://www.worldwater.org/conflict/map/
12	*Very High*	**Iran and Afghanistan are feuding over the Helmand River. The water wars have no end in sight.**
		https://www.atlanticcouncil.org/blogs/iransource/iran-afghanistan-taliban-water-helmand/
North Korea Highly Likely to Improve Warhead Delivery Capability by 2027		
##	*Trust Scale*	*Article*
1	*Very High*	**Missiles of North Korea**
		https://missilethreat.csis.org/country/dprk/
2	*Very High*	**Ground-based Midcourse Defense – Media Resources**
		https://missilethreat.csis.org/ground-based-midcourse-defense-resources/

3	*High*	**North Korea Events of 2023**
		https://www.hrw.org/world-report/2024/country-chapters/north-korea
4	*Very High*	**North Korea's Nuclear Weapons and Missile Programs**
		https://sgp.fas.org/crs/nuke/IF10472.pdf
5	*High*	**North Korea says it tested solid-fuel missile tipped with hypersonic weapon**
		https://www.nbcnews.com/news/world/north-korea-says-tested-solid-fuel-missile-tipped-hypersonic-weapon-rcna133900
6	*Very High*	**Korea, North**
		https://www.cia.gov/the-world-factbook/countries/korea-north/
7	*High*	**The US, South Korea and Japan conduct naval drills in a show of strength against North Korea**
		https://apnews.com/article/us-south-korea-japan-naval-exercise-north-korea-e04d3adef36799f6f31b3ba2643ff2fe
8	*High*	**Fearless, factual, global news**
		https://www.theguardian.com/us-news/2022/nov/03/north-korea-nuclear-attack-us-kim-regime-lloyd-austin
9	*High*	**North Korea: China urges Trump not to worsen situation**
		https://www.bbc.com/news/world-asia-40909468
10	*High*	**Who Would Win in a War Between the United States and North Korea**
		https://bigthink.com/technology-innovation/who-will-win-in-a-war-between-the-united-states-and-north-korea/
11	*High*	**A Timeline of North Korea's Missile Launches and Nuclear Detonations**
		https://www.bloomberg.com/politics/articles/2017-04-16/north-korea-missile-launches-nuclear-detonations-timeline
12	*Very High*	**What to Know About Sanctions on North Korea**
		https://www.cfr.org/backgrounder/north-korea-sanctions-un-nuclear-weapons
13	*Very High*	**North Korea's Foreign Affairs Hit an Inflection Point**
		https://worldview.stratfor.com/article/north-koreas-foreign-affairs-hit-inflection-point
14	*Very High*	**Geopolitical Intelligence**
		https://www.ranenetwork.com/platform/products/geopolitical-intelligence
15	*Very High*	**Some Historical Perspective**
		https://www.pbs.org/wgbh/pages/frontline/shows/kim/them/historical.html
16	*High*	**Characterizing the North Korean Nuclear Missile Threat**
		https://www.rand.org/pubs/technical_reports/TR1268.html
17	*High*	**North Korea**
		https://www.brookings.edu/regions/asia-the-pacific/north-korea/
18	*High*	**If you want peace, prepare for war — and diplomacy**
		https://www.brookings.edu/articles/if-you-want-peace-prepare-for-war-and-diplomacy/
19	*High*	**Report to Congress on North Korea's Nuclear Weapons and Missile Programs**
		https://news.usni.org/2023/01/26/report-to-congress-on-north-koreas-nuclear-weapons-and-missile-programs
North Korea Highly Likely to Continue Self-Sustaining Nuclear Program through 2027 and Beyond and Foreign Support Highly Unlikely to Bolster North Korea's Nuclear Program through 2027 and Beyond		

##	*Trust Scale*	*Article*
1	*Very High*	**A COMPREHENSIVE HISTORY OF NORTH KOREA'S NUCLEAR PROGRAM**
		https://cisac.fsi.stanford.edu/content/cisac-north-korea
2	*Very High*	**These 28 companies are building nuclear weapons: ICAN**
		https://www.pressenza.com/2019/05/these-28-companies-are-building-nuclear-weapons-ican/
3	*Very High*	**Meet the Private Corporations Building Our Nuclear Arsenal**
		https://www.thenation.com/article/society/meet-the-private-corporations-building-our-nuclear-arsenal/
4	*Very High*	**Top 25 Nuclear Research and Development Companies**
		https://www.inven.ai/company-lists/top-25-nuclear-research-and-development-companies
5	*Very High*	**North Korea Nuclear Overview**
		https://www.nti.org/analysis/articles/north-korea-nuclear/
6	*Very High*	**Nuclear power in North Korea**
		https://en.wikipedia.org/wiki/Nuclear_power_in_North_Korea
7	*Very High*	**North Korea tests underwater nuclear weapon amid soaring tensions with South**
		https://www.msn.com/en-gb/news/world/north-korea-tests-underwater-nuclear-weapon-amid-soaring-tensions-with-south/ar-BB1gVHnr
8	*Very High*	**North Korea is not a treasure ship**
		https://weekly.chosun.com/news/articleView.html?idxno=13321
9	*Very High*	**Profiting from Proliferation? North Korea's Exports of Missile and Nuclear Technology**
		https://rusi.org/explore-our-research/publications/occasional-papers/profiting-proliferation-north-koreas-exports-missile-and-nuclear-technology
10	*Very High*	**North Korea training, providing weapons to Hamas, Hezbollah, and Houthis**
		https://www.msn.com/en-us/news/world/north-korea-training-and-providing-arms-to-hamas-hezbollah-and-houthis-report/ar-AA1n6HYj
11	*Very High*	**Assessing N. Korea's efforts to encourage private business**
		https://www.dailynk.com/english/assessing-north-korea-efforts-encourage-private-business/
12	*Very High*	**Private sector overtakes state as North Korea's top economic actor under Kim -SKorea**
		https://www.reuters.com/markets/asia/private-sector-overtakes-state-north-koreas-top-economic-actor-under-kim-skorea-2021-12-16/
13	*Very High*	**North Korea's private sector overtakes state for first time under Kim Jong-un**
		https://www.independent.co.uk/asia/east-asia/north-korea-kim-jong-un-private-sector-b1977299.html
14	*Very High*	**The Markets: Private Economy and Capitalism in North Korea?**
		https://beyondparallel.csis.org/markets-private-economy-capitalism-north-korea/
15	*Very High*	**UF-LED GROUP DEVELOPS NEW TOOLS TO TRACK ILLICIT NUCLEAR MATERIALS**
		https://mse.ufl.edu/uf-led-group-develops-new-tools-to-track-illicit-nuclear-materials/

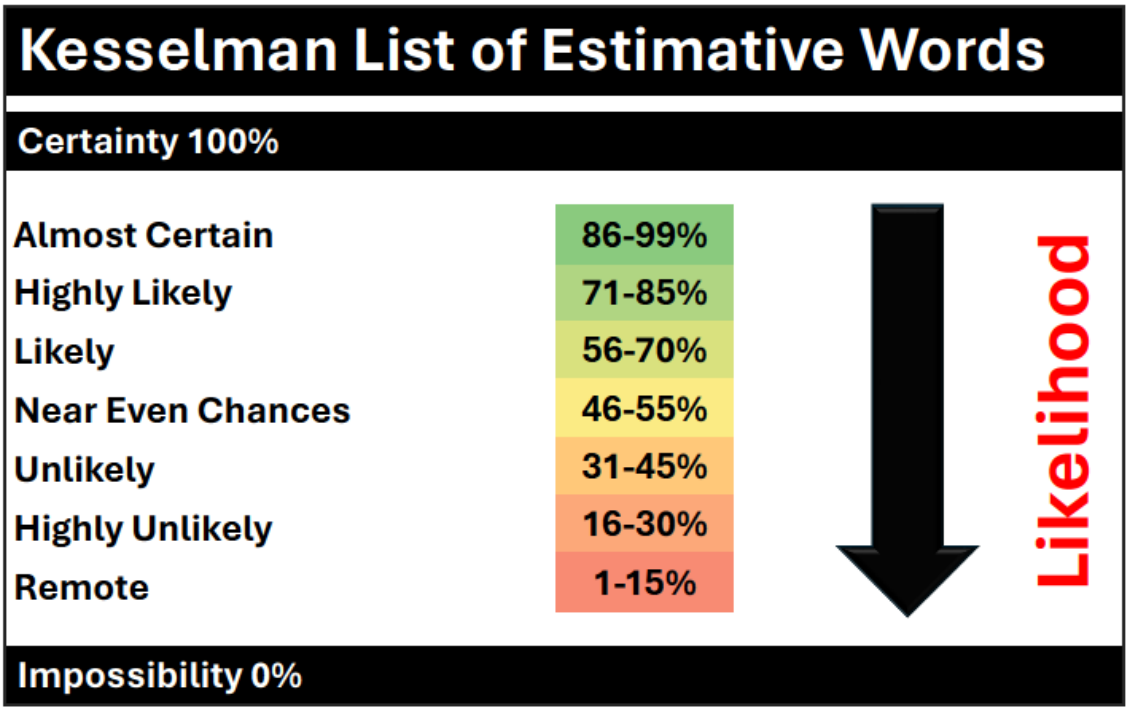
16	*Very High*	**What to Know About Doing Business in North Korea**
		https://thediplomat.com/2018/08/what-to-know-about-doing-business-in-north-korea/
17	*Very High*	**Transparency International: About**
		https://www.transparency.org/en/about
18	*Very High*	**Planned U.S.-North Korea Talks Postponed**
		https://www.armscontrol.org/blog/2018-11-16/north-korea-denuclearization-digest-november-16-2018
19	*Very High*	**IAEA Releases Annual Data on Illicit Trafficking of Nuclear and other Radioactive Material**
		https://www.iaea.org/newscenter/pressreleases/iaea-releases-annual-data-on-illicit-trafficking-of-nuclear-and-other-radioactive-material
20	*Very High*	**The Prospects for North Korea-Russia Nuclear Cooperation**
		https://thediplomat.com/2023/11/the-prospects-for-north-korea-russia-nuclear-cooperation/
21	*Very High*	**Revisiting History: North Korea and Nuclear Weapons**
		https://www.wilsoncenter.org/event/revisiting-history-north-korea-and-nuclear-weapons
North Korea's Artificial Intelligence Capability Growth Highly Likely by 2027 and Beyond		
##	*Trust Scale*	*Article*
1	*Very High*	**North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications**
		https://www.38north.org/2024/01/north-koreas-artificial-intelligence-research-trends-and-potential-civilian-and-military-applications/
2	*Very High*	**Making North Korea's 'Silver Star Go' Hero**
		https://www.joongang.co.kr/article/1755875#home
3	*Very High*	**North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications**
		https://nonproliferation.org/north-koreas-artificial-intelligence-research-trends-and-potential-civilian-and-military-applications/
4	*Very High*	**NORTH KOREA'S ADVANCEMENTS IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING**
		https://www.cryptopolitan.com/north-korea-advancements-in-ai-and-ml/
5	*High*	**North Korea's AI-Powered Cyberwarfare Program: A New Threat to the World**
		https://www.gizmochina.com/2023/10/19/north-korea-ai-cyberattacks/
6	*Very High*	**Will Artificial Intelligence Hone North Korea's Cyber "All-Purpose Sword"?**
		https://keia.org/publication/will-artificial-intelligence-hone-north-koreas-cyber-all-purpose-sword/
7	*High*	**Elon Musk says AI could lead to third world war**
		https://www.theguardian.com/technology/2017/sep/04/elon-musk-ai-third-world-war-vladimir-putin
8	*High*	**Elon Musk warns A.I. could create an 'immortal dictator from which we can never escape'**
		https://www.cnbc.com/2018/04/06/elon-musk-warns-ai-could-create-immortal-dictator-in-documentary.html
9	*Very High*	**U.S. INDO-PACIFIC COMMAND POSTURE**

		https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/2023%20INDOPACOM%20Statement%20for%20the%20Record.pdf
10	*Moderate*	**Putin to boost AI work in Russia to fight a Western monopoly he says is 'unacceptable and dangerous'**
		https://apnews.com/article/putin-russia-artificial-intelligence-3098b4f5205785f1b8281b34f13bff92
11	*Moderate*	**Putin says West cannot have AI monopoly so Russia must up its game**
		https://www.reuters.com/technology/putin-approve-new-ai-strategy-calls-boost-supercomputers-2023-11-24/
12	*Very High*	**ARTIFICIAL INTELLIGENCE AND AUTONOMY IN RUSSIA**
		https://www.cna.org/centers-and-divisions/cna/sppp/russia-studies/artificial-intelligence-and-autonomy-in-russia
13	*Moderate*	**Putin Wants Russia to Win the Artificial Intelligence Race. Here's Why it Won't**
		https://www.themoscowtimes.com/2023/11/14/putin-wants-russia-to-win-the-artificial-intelligence-race-heres-why-it-wont-a83103
14	*Very High*	**"AI weapons" in China's military innovation**
		https://www.brookings.edu/articles/ai-weapons-in-chinas-military-innovation/
15	*Very High*	**How Does China Aim to Use AI in Warfare?**
		https://thediplomat.com/2021/12/how-does-china-aim-to-use-ai-in-warfare/
16	*Very High*	**How China is using AI for warfare**
		https://cset.georgetown.edu/article/how-china-is-using-ai-for-warfare/
17	*Moderate*	**The next arms race: China leverages AI for edge in future wars**
		https://www.japantimes.co.jp/news/2023/04/20/asia-pacific/china-ai-future-wars/
18	*Moderate*	**The Real AI Weapons Are Drones, Not Nukes**
		https://www.theatlantic.com/ideas/archive/2024/02/artificial-intelligence-war-autonomous-weapons/677306/

North Korea's Profit-Focused Cybercrime Capabilities Almost Certain to Increase By 2027 and Beyond		
##	*Trust Scale*	*Article*
1	*Very High*	**Korea Quantum Computing and IBM Collaborate to Bring IBM watsonx and Quantum Computing to Korea**
		https://www.prnewswire.com/news-releases/korea-quantum-computing-and-ibm-collaborate-to-bring-ibm-watsonx-and-quantum-computing-to-korea-302047206.html
2	*Moderate*	**North Korea Cybercrimes Undermine Sanctions and Threaten America**
		https://www.heritage.org/cybersecurity/commentary/north-korea-cybercrimes-undermine-sanctions-and-threaten-america
3	*Very High*	**Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations**
		https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government
4	*Very High*	**Why Is North Korea So Good at Cybercrime?**
		https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/

5	*Very High*	**What Will North Korean Cybercrime Look Like in 2022?** https://thediplomat.com/2021/12/what-will-north-korean-cybercrime-look-like-in-2022/
6	*Moderate*	**PASQAL, The Korea Advanced Institute Of Science And Technology (KAIST), And Daejeon City Forge Quantum Partnership** https://thequantuminsider.com/2024/02/07/pasqal-the-korea-advanced-institute-of-science-and-technology-kaist-and-daejeon-city-forge-quantum-partnership/
7	*Low*	**North Korean hackers are getting away with a lot less crypto even as theft attempts rise** https://www.msn.com/en-us/money/markets/north-korean-hackers-are-getting-away-with-a-lot-less-crypto-even-as-theft-attempts-rise/ar-BB1hfDKI
8	*Moderate*	**Yoon explores Korea's strategies for quantum technology** https://www.koreatimes.co.kr/www/nation/2023/01/356_343948.html
9	*Moderate*	**North Korea touts quantum computing for economic development** https://www.upi.com/Top_News/World-News/2019/09/05/North-Korea-touts-quantum-computing-for-economic-development/4411567702534/
10	*Very High*	**Mapping Major Milestones in the Evolution of North Korea's Cyber Program** https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/
11	*Moderate*	**AI in Cybersecurity** https://www.geeksforgeeks.org/ai-in-cybersecurity/#
12	*Very High*	**Artificial intelligence (AI) cybersecurity** https://www.ibm.com/ai-cybersecurity
13	*Moderate*	**North Korea's state hacking program is varied, fluid, and nimble** https://www.csoonline.com/article/657312/north-koreas-state-hacking-program-is-varied-fluid-and-nimble.html
14	*Very High*	**North Korea's Cyber Capabilities** https://www.csis.org/programs/korea-chair/projects/korea-chair-project-archive/north-koreas-cyber-capabilities
15	*Very High*	**US, Japan, South Korea step up efforts to counter North Korea cyber-threats** https://www.aljazeera.com/news/2023/12/9/us-japan-south-korea-launch-new-efforts-to-counter-n-korea-cyber-threats
16	*Moderate*	**North Korea's Cyber Capabilities and Strategy** https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0

Annex C – Kesselman List of Estimative Words



*Note, Kesselman utilizes "Chances a Little Better [or Less]"; team replaced this with Near Even Chances for Readability

Annex D – Innovation Multi-Criteria Decision Analysis

Evaluation of contemporary conflict innovations using nominative group technique to rank them according to their likelihood of impacting various operational and enterprise components.

Innovations	Operational Component Evaluation: Joint Warfighting Functions								Enterprise Component Evaluation: Technological, Economic, Strategic, Ethical, and Environmental Factors								Combined Evaluation		Outcome	% of Scoring
Rank (negative inverse): 0 - None 25 - Little 50 - Medium 75 - Mostly 100 - Total	Intelligence	Movement & Maneuver	Fires	Information	Protection	Sustainment	Command & Control	Total	Rank	Cost-effectiveness	Risk and Uncertainty	Ethical and Legal Implications	Technological Readiness	Interoperability and Integration	Strategic Alignment	Performance Matrix	Total	Rank	Rank	
Weight	100%	100%	100%	100%	100%	100%	100%			100%	100%	100%	100%	100%	100%	100%				
Adaptive Integration *(Blending Not Hiding)*	100	100	95	30	85	35	50	**495**	**1**	70	-40	0	25	30	100	55	**240**	**2**	**735**	**1**	*Unprecedented Battlefield Visibility*	*22%*
Artificial Intelligence	85	55	60	80	30	60	45	**415**	**2**	100	-70	-60	45	35	90	50	**190**	**3**	**605**	**2**	*Rapid, Technology-Enabled Warfare*	*18%*
Hybrid Warfare *(Rapid Influence of Citizens)*	85	40	65	90	45	15	30	**370**	**3**	65	-50	-40	70	60	60	25	**190**	**3**	**560**	**4**	*Unprecedented Battlefield Visibility*	*17%*
Autonomous Systems	60	55	50	30	50	45	10	**300**	**4**	75	-50	-55	70	50	100	75	**265**	**1**	**565**	**3**	*Rapid, Technology-Enabled Warfare*	*17%*
Water Warfare	20	45	20	20	45	80	5	**235**	**5**	20	-35	-70	45	70	10	30	**70**	**6**	**305**	**6**	*Vulnerable Homeland*	*9%*
Sixth Domain *(Private-Sector Involvement)*	45	15	30	45	35	35	25	**230**	**6**	100	-90	-55	40	25	50	25	**95**	**5**	**325**	**5**	*Lower Barriers to Entry of Participants*	*10%*
5th Generation Warfare *(Citizen Supplemented)*	45	0	15	50	15	10	5	**140**	**7**	80	-100	-45	30	35	10	30	**40**	**7**	**180**	**7**	*Lower Barriers to Entry of Participants*	*5%*

Definitions	
Cost-effectiveness:	Upfront Costs appropriate? Long-Term operational/maintenance costs? Return on Investment?
Risk and Uncertainty:	New Vulnerabilities/Risks introduced with innovation? Mitigation strategies available/feasible?
Ethical and Legal Implications:	Ethical concerns with usage? Complies with country/international laws, treaties, regulations?
Technological Readiness:	Improves Readiness/Capabilities/Defensive-Offensive Operations?
Interoperability and Integration:	Innovation is/can be interoperable or integrated with doctrine, systems, processes?
Technological Feasibility:	Current state of development or readiness for deployment?
Strategic Alignment:	Innovation aligns with or supports mission or strategic objectives?
Stakeholder Impact:	Impact on military personnel (training, roles)? Impact on civilian population (daily lives, safety, privacy)?
Performance Matrix:	Effectiveness of improving warfighting functions? Reliability and consistency under various conditions?

Outcome Scoring		
Outcome	**Score**	**Rank**
Unprecedented Battlefield Visibility	1,295	1
Rapid, Technology-Enabled Warfare	1,170	2
Vulnerable Homeland	305	4
Lower Barriers to Entry of Participants	505	3
	3,275	
%%	*40%*	
	36%	
	9%	
	15%	

Scoring Method: Nominal Group Technique - The nominal group technique (NGT) is a structured method of brainstorming within a group setting designed to encourage partic/paton from all group members. Scores are average of team members.

Annex E – Presentation Slides

Future Warfare:
Everyone is a Player
Everything is a Target

LTC Joe Bell

COL John Cooper

LTC Kris Hinds

LtCol Erik Keim

LTC Michael “Neal” Miller

Faculty Advisor: Dr. Kathleen Moore

Sullivan's TRAVELS

22APR24

Kesselman List of Estimative Words

Certainty 100%

Almost Certain	86-99%
Highly Likely	71-85%
Likely	56-70%
Near Even Chances	46-55%
Unlikely	31-45%
Highly Unlikely	16-30%
Remote	1-15%

Likelihood

Impossibility 0%

**Note, Kesselman utilizes "Chances a Little Better [or Less]"; team replaced this with Near Even Chances for readability*

How will innovations from contemporary conflicts likely shape the future dynamics of warfare, and what does it mean for Large Scale Combat Operations (LSCO) and pacing threats by 2035?

It is **highly likely (71-86%)** that innovations from recent conflicts will more fully integrate a diverse array of actors into future conflict, due to increased entry points enabled by:

- Unprecedented Visibility
- Rapid Technology Implementation
- Lower Barriers to Entry
- Vulnerable Homelands

Despite the traditional role of militaries during conflict, the ubiquity of tech and the treatment of conflict as a testing bed (sandbox) increases the rapid implementation of material and non-material applications by any party.

Everyone is a Player
Everything is a Target

“Conflict as a Sandbox”

Future Warfare:

Everyone is a Player; Everything is a Target

Team
LTC Joseph "Joe" Bell (USA, Aviation)
COL John Cooper (USA, Human Resources)
LTC Kristine "Kris" Hinds (USAR, Logistics)
LtCol Erik Keim (USMC, Comms)
LTC Michael "Neal" Miller (USAR, Logistics)

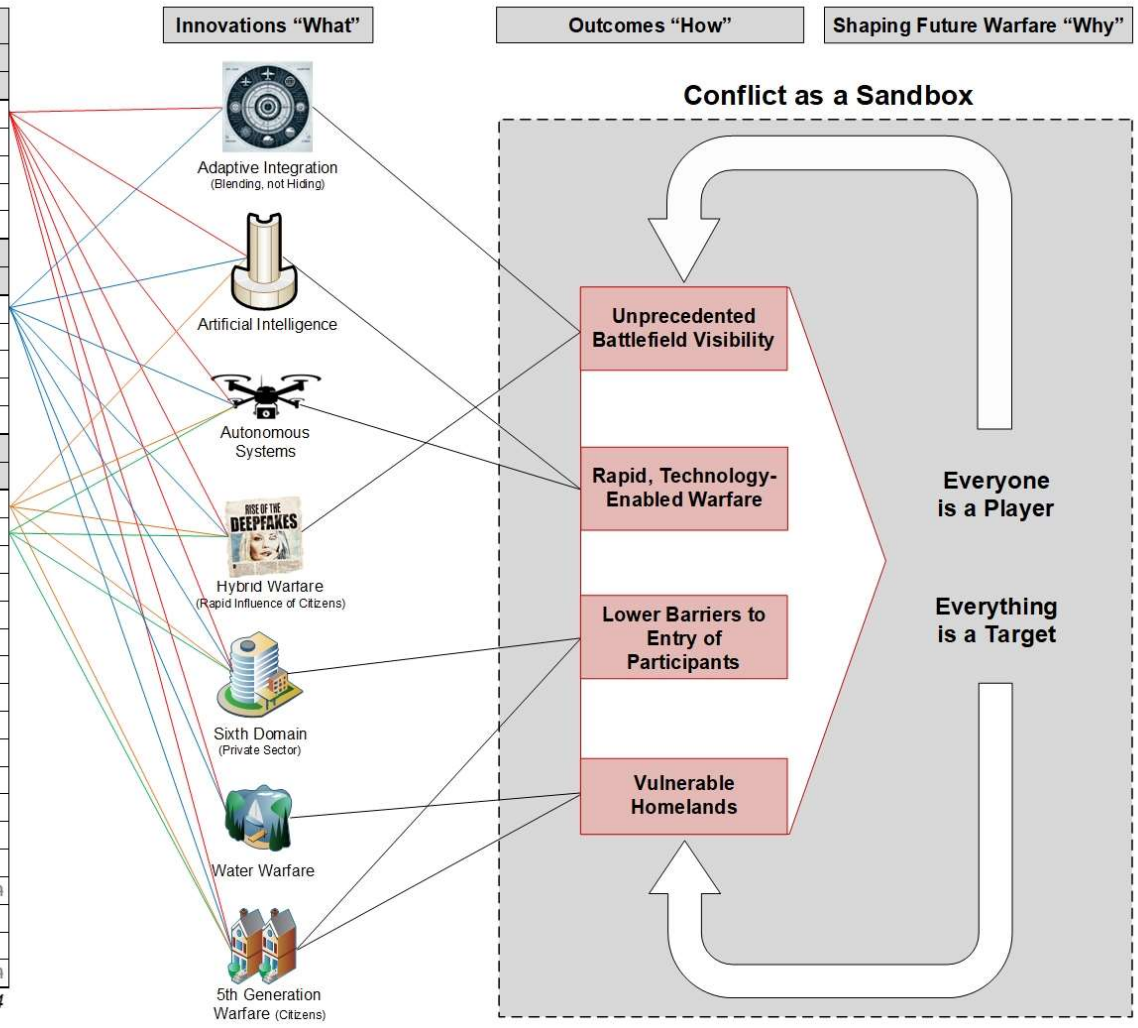
Faculty Advisor: Dr. Kathleen Moore

How will innovations from contemporary conflicts likely shape the future dynamics of warfare, and what does it mean for Large Scale Combat Operations (LSCO) and pacing threats by 2035?

Council on Foreign Relations: Global Conflict Tracker

##	Conflict	Category
Critical Impact on United States		
1	War in Ukraine	Interstate
2	Territorial Disputes in the South China Sea	Territorial Dispute
3	Confrontation Over Taiwan	Interstate
4	Confrontation With Iran	Interstate
5	North Korea Crisis	Interstate
Significant Impact on United States		
6	Israeli-Palestinian Conflict	Territorial Dispute
7	Conflict Between India and Pakistan	Interstate
8	Criminal Violence in Mexico	Criminal Violence
9	Instability in Haiti	Political Instability
10	Instability in the Northern Triangle	Political Instability
Limited Impact on United States		
11	War in Yemen	Civil War
12	Nagorno-Karabakh Conflict	Territorial Dispute
13	Conflict Between Turkey and Armed Kurdish Groups	Territorial Dispute
14	Civil War in Myanmar	Civil War
15	Civil War in Sudan	Civil War
16	Conflict in Syria	Civil War
17	Civil Conflict in Libya	Civil War
18	Conflict in the Central African Republic	Civil War
19	Conflict in Ethiopia	Political Instability
20	Conflict in the Democratic Republic of Congo	Political Instability
21	Instability in Afghanistan	Political Instability
22	Instability in Iraq	Political Instability
23	Instability in Lebanon	Political Instability
24	Instability in Pakistan	Political Instability
25	Violent Extremism in the Sahel	Transnational Terrorism
26	Instability in South Sudan	Political Instability
27	Venezuela Crisis	Political Instability
28	Conflict With Al-Shabaab in Somalia	Transnational Terrorism

Source: https://www.cfr.org/global-conflict-tracker *As of 8 April 2024*



Council on Foreign Relations: Global Conflict Tracker		
Critical Impact on United States		
##	Conflict	Category
1	**War in Ukraine**	**Interstate**
2	~~Territorial Disputes in the South China Sea~~	~~Territorial Dispute~~
3	~~Confrontation Over Taiwan~~	~~Interstate~~
4	~~Confrontation With Iran~~	~~Interstate~~
5	~~North Korea Crisis~~	~~Interstate~~
Significant Impact on United States		
##	Conflict	Category
6	**Israeli-Palestinian Conflict**	**Territorial Dispute**
7	~~Conflict Between India and Pakistan~~	~~Interstate~~
8	~~Criminal Violence in Mexico~~	~~Criminal Violence~~
9	~~Instability in Haiti~~	~~Political Instability~~
10	~~Instability in the Northern Triangle~~	~~Political Instability~~
Limited Impact on United States		
##	Conflict	Category
11	**War in Yemen**	**Civil War**
12	**Nagorno-Karabakh Conflict**	**Territorial Dispute**
13	~~Conflict Between Turkey and Armed Kurdish Groups~~	~~Territorial Dispute~~
14	~~Civil War in Myanmar~~	~~Civil War~~
15	~~Civil War in Sudan~~	~~Civil War~~
16	~~Conflict in Syria~~	~~Civil War~~
17	~~Civil Conflict in Libya~~	~~Civil War~~
18	~~Conflict in the Central African Republic~~	~~Civil War~~
19	~~Conflict in Ethiopia~~	~~Political Instability~~
20	~~Conflict in the Democratic Republic of Congo~~	~~Political Instability~~
21	~~Instability in Afghanistan~~	~~Political Instability~~
22	~~Instability in Iraq~~	~~Political Instability~~
23	~~Instability in Lebanon~~	~~Political Instability~~
24	~~Instability in Pakistan~~	~~Political Instability~~
25	~~Violent Extremism in the Sahel~~	~~Transnational Terrorism~~
26	~~Instability in South Sudan~~	~~Political Instability~~
27	~~Venezuela Crisis~~	~~Political Instability~~
28	~~Conflict With Al-Shabaab in Somalia~~	~~Transnational Terrorism~~
Source: https://www.cfr.org/global-conflict-tracker		*As of 8 April 2024*

*28 Total Conflicts

<u>Conflict Criteria</u>
Within 5 years
Military Casualties > 100
Significant Innovation and Impact to LSCO

<u>Eliminated</u>
Territorial Disputes
Civil War or Political Instability

<u>Remaining</u>
Ukraine-Russia
Israel-Hamas
Azerbaijan-Armenia
Houthis-Red Sea

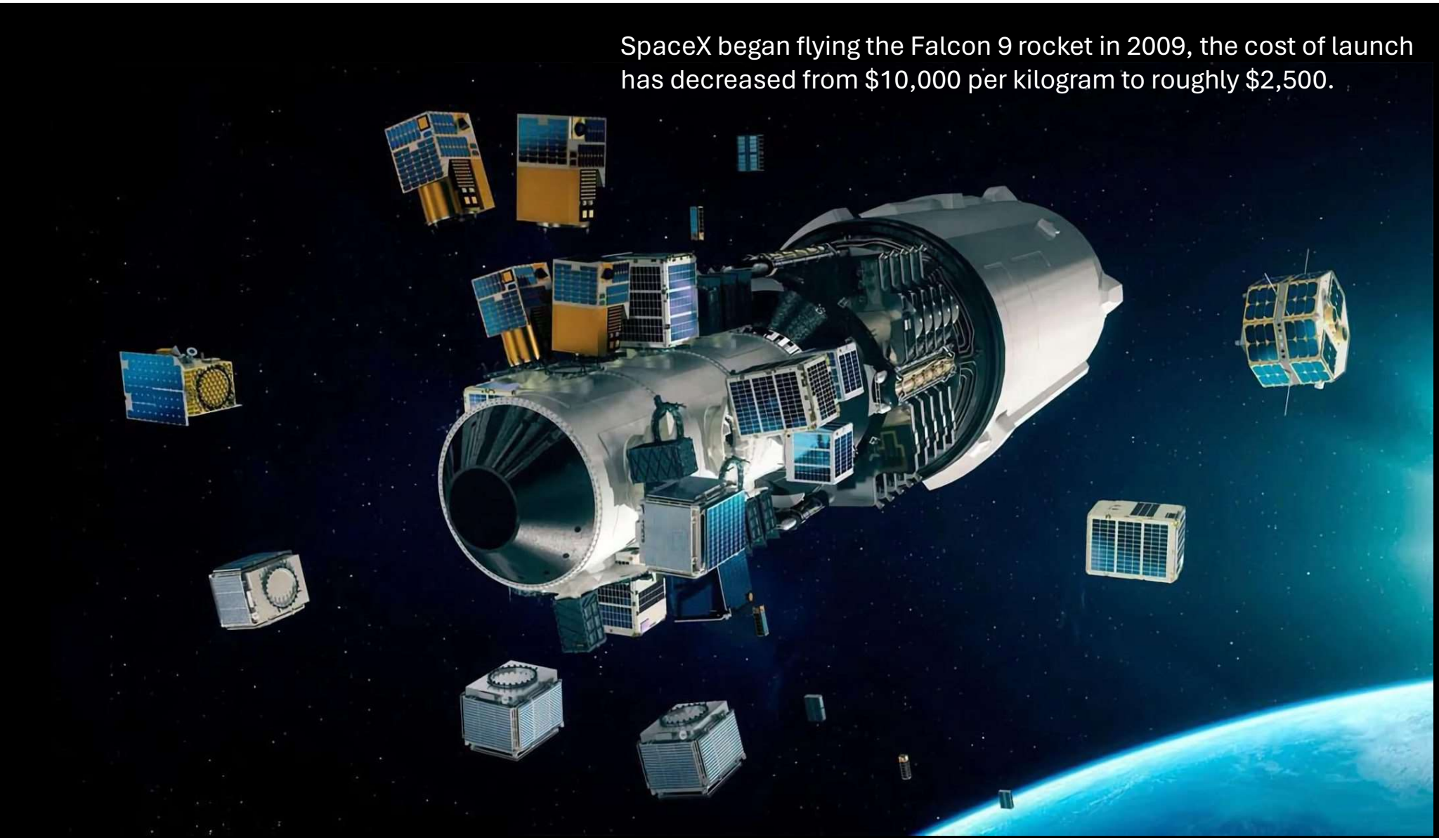
Unprecedented Battlefield Visibility

It is highly likely that transformations driven by advancements in ISR, rapid production of equipment, and accessibility of space and communications will make covert operations increasingly challenging.

Key innovations

- Adaptive Integration
- Hybrid Warfare (Rapid Influence of Citizens)

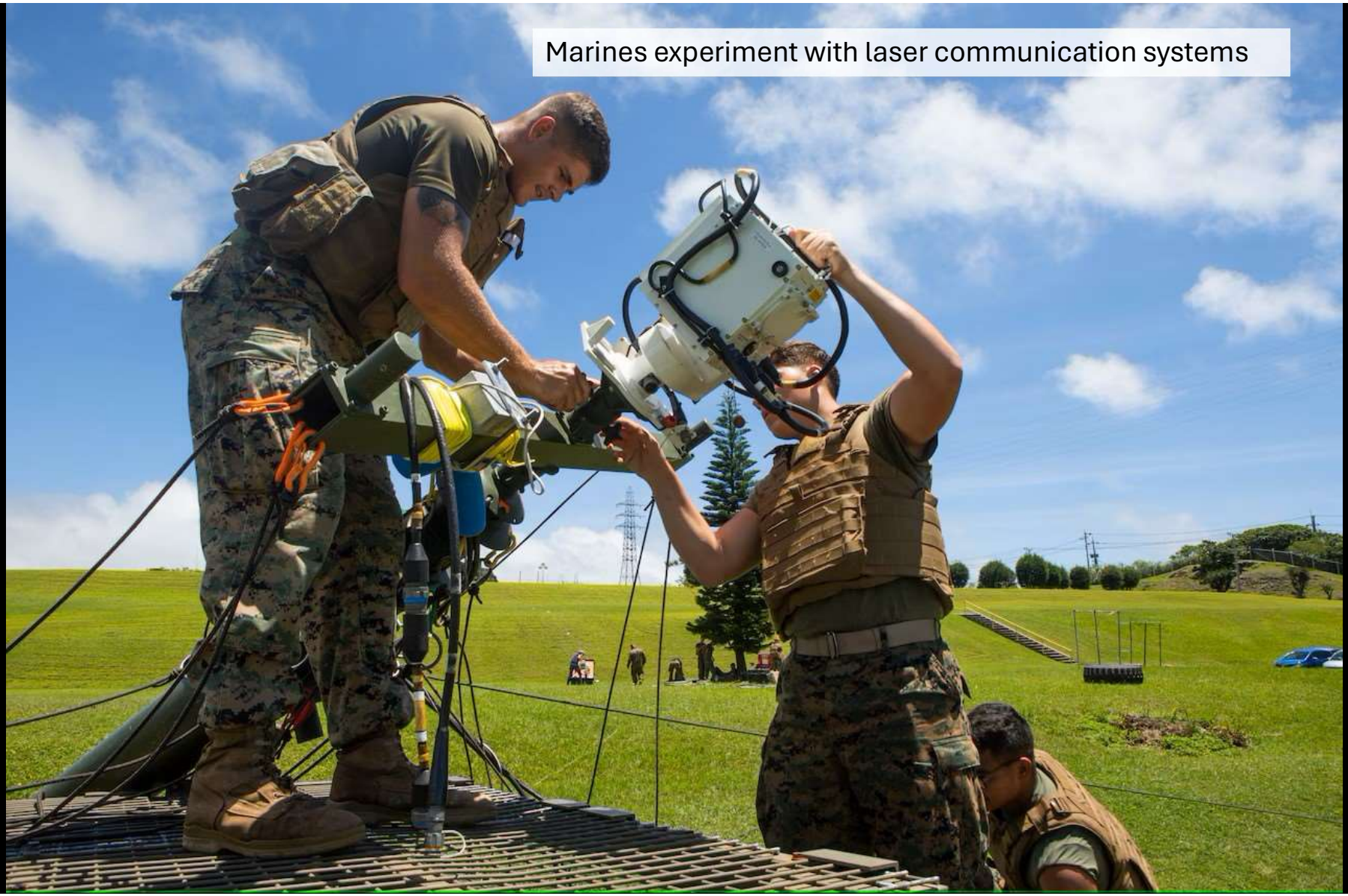
Some of the 3,000 drones produced by Ukraine every day


SpaceX began flying the Falcon 9 rocket in 2009, the cost of launch has decreased from $10,000 per kilogram to roughly $2,500.

Maxar satellite image of the southern end of a large Russian military convoy near Antonov Airport near Kyiv

Planet Labs image of Ukraine's Chuhuiv Airbase

A radio direction finding device is used to locate the source of radio transmissions


Marines experiment with laser communication systems

The divergence of laser compared to microwave communication systems

FSO - Free Space Optics uses laser light instead of radio waves to transmit data


African Maasi herder using a cellphone

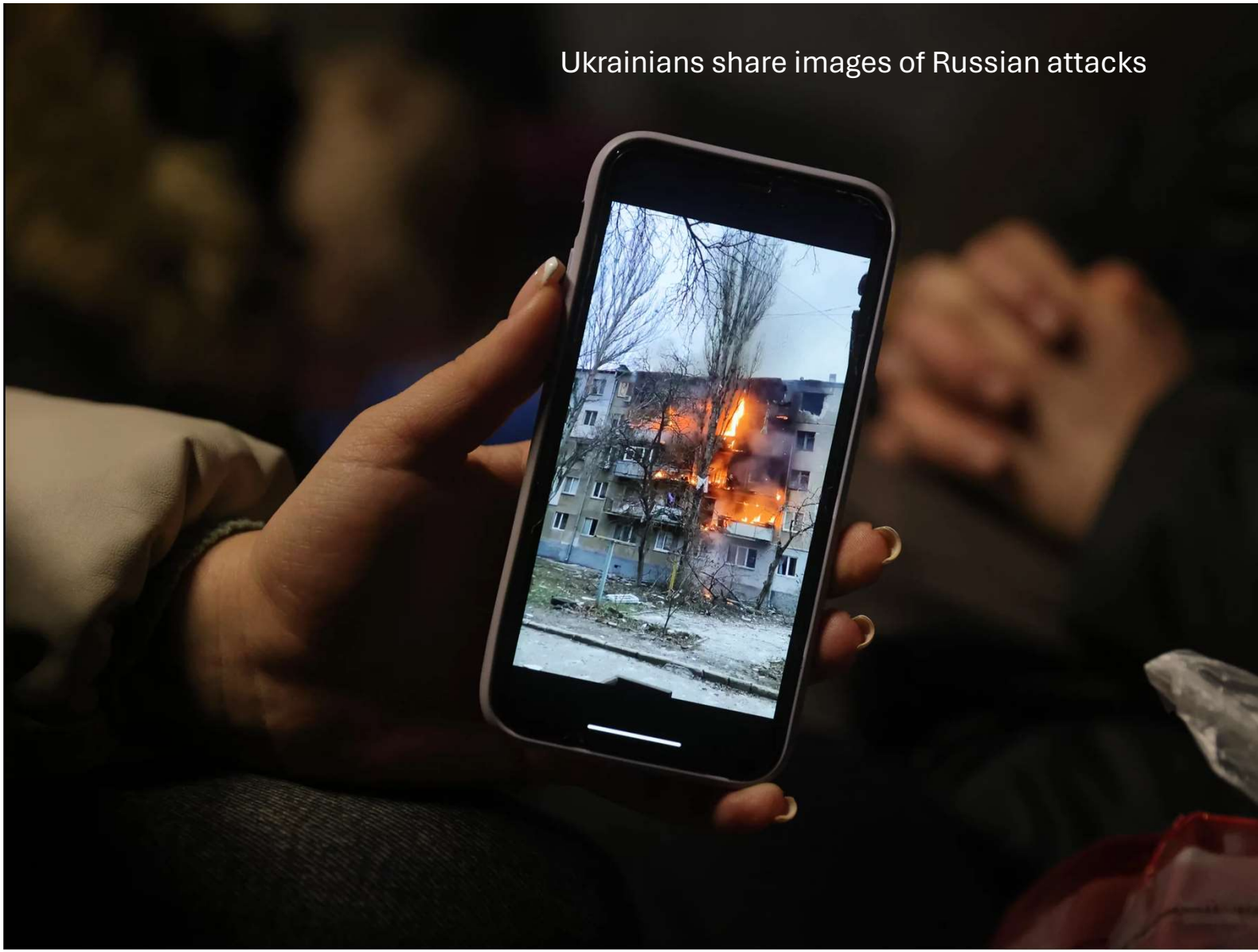
Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine

Attack On Europe: Documenting Ukrainian Equipment Losses During The Russian Invasion Of Ukraine

A Monument Of Victory: The Bayraktar TB2 Kill List

List Of Aircraft Losses During The Russian Invasion Of Ukraine

Answering The Call: Heavy Weaponry Supplied To Ukraine



Rapid, Technology-Enabled Warfare

Rapid employment of information warfare, precision targeting, and tactical maneuver execution are **highly likely** to shape future warfare.

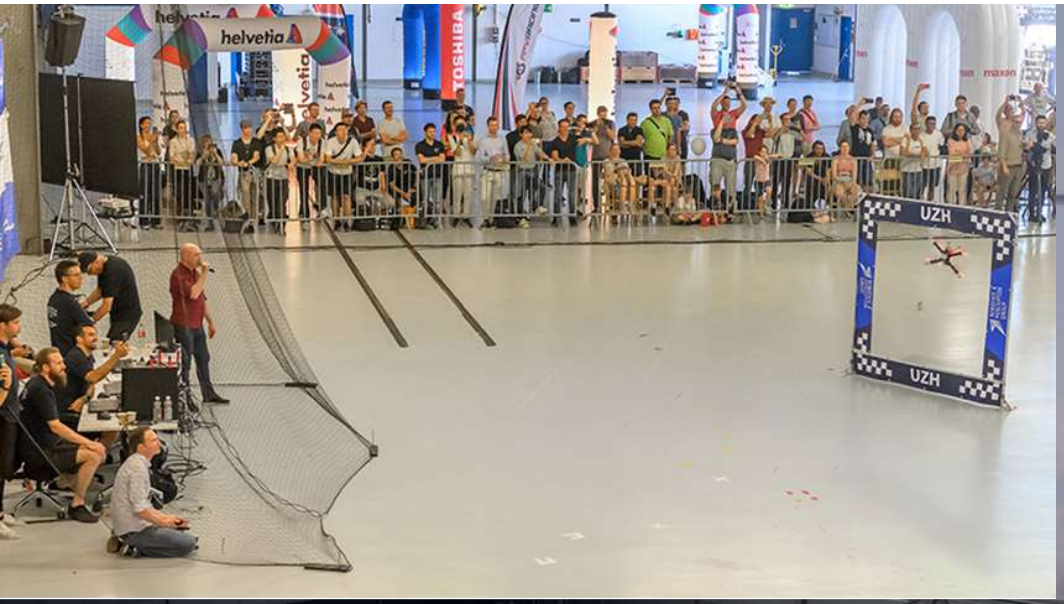
Key innovations

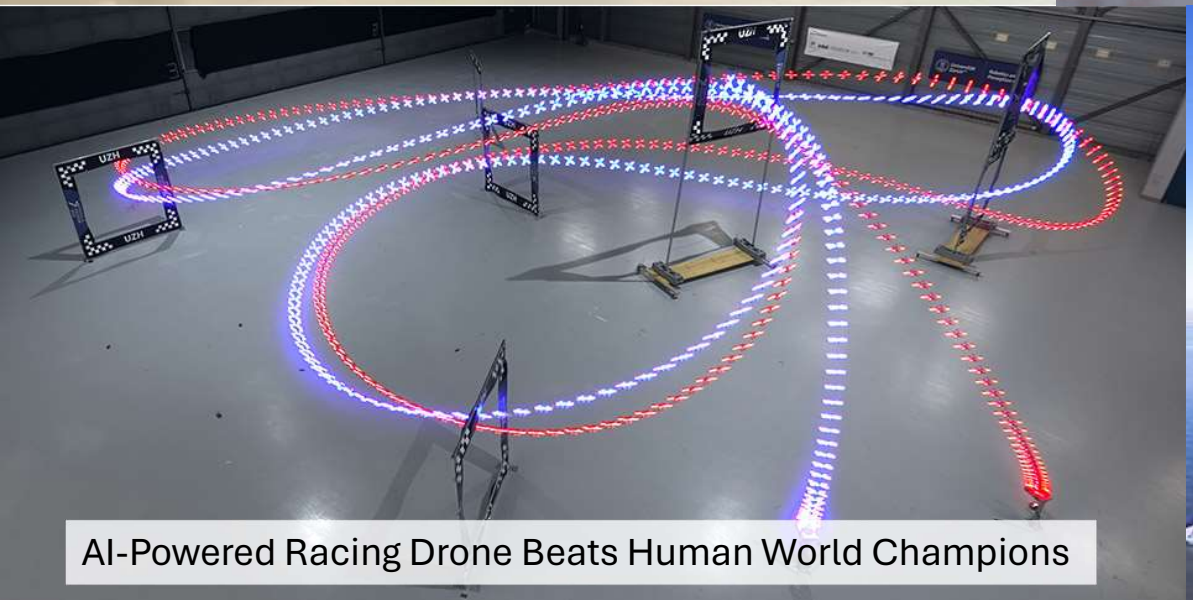
- Artificial Intelligence
- Autonomous Systems


REAL
FAKE


Lavender/Gospel recommendations
DEMOCRACY NOW!
Israel's AI-Generated Kill Lists

Moments before a Ukrainian drone hits Russian troops





AI-Powered Racing Drone Beats Human World Champions

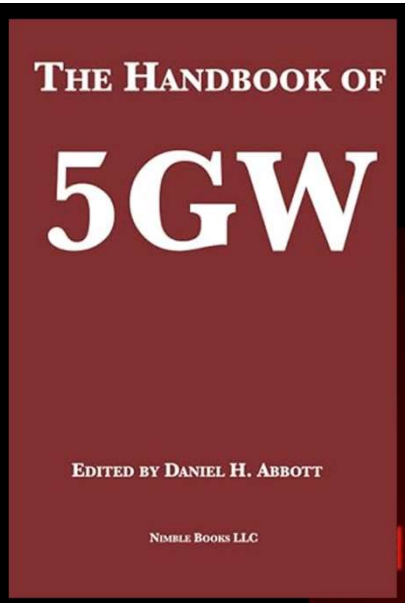
Low Barriers to Entry for Participants

It is highly likely that an increased array of non-traditional military actors and ways in which to target will play pivotal roles in conflict and pre-conflict dynamics by leveraging commercially available technologies to conduct operations, intelligence gathering, and public opinion influence.

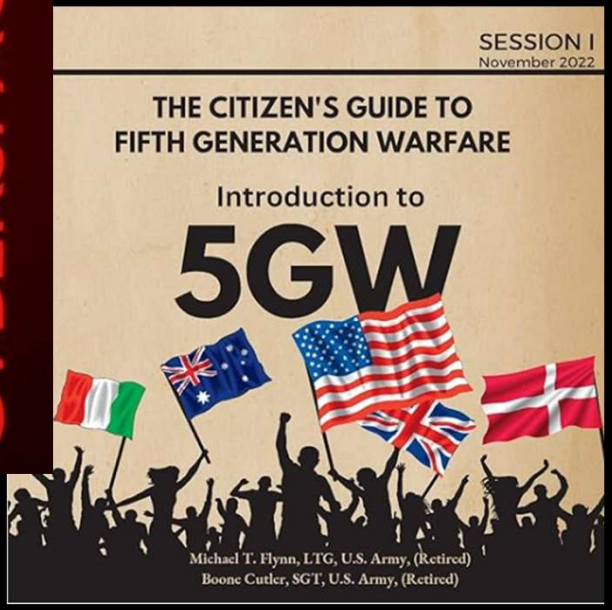
This allows broader conflict participation and agenda-driven actors to rapidly develop innovative technologies

Key innovations

- Sixth Domain (Private Sector)
- Fifth Generation Warfare (Citizen Supplemented)

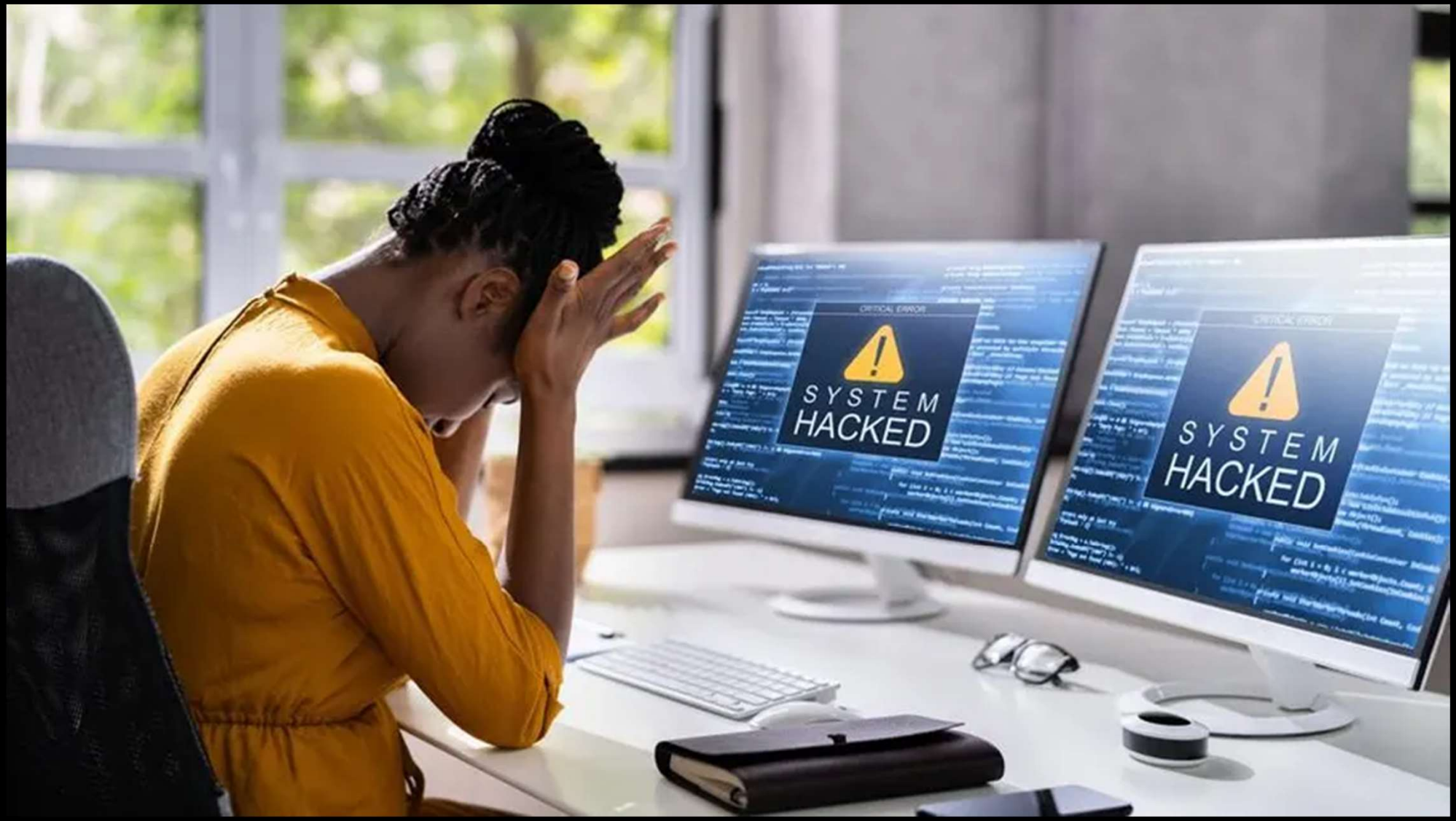


5th Generation War and Global Challenges - Stratheia




Digital Dopamine
How iTech is Transforming Our Minds


The smartphone is the modern-day hypodermic needle, delivering digital dopamine 24/7 for a wired generation.


SYSTEM
HACKED
SYSTEM
HACKED

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

REPORT LAUNCH

THE SIXTH DOMAIN AND THE ROLE OF THE PRIVATE SECTOR

Friday, April 26 | 1:00 p.m. (ET)

Elon Musk

Elon Musk ordered Starlink to be turned off during Ukraine offensive, book says

Biography alleges Musk told engineers to turn off communications network to hobble Ukraine drone attack on Russian warships

Musk reportedly referred to the attack as a 'mini Pearl Harbor'. Photograph: Alain Jocard/AFP/Getty Images

Julian Borger *in Washington*

Thu 7 Sep 2023 23.14 BST

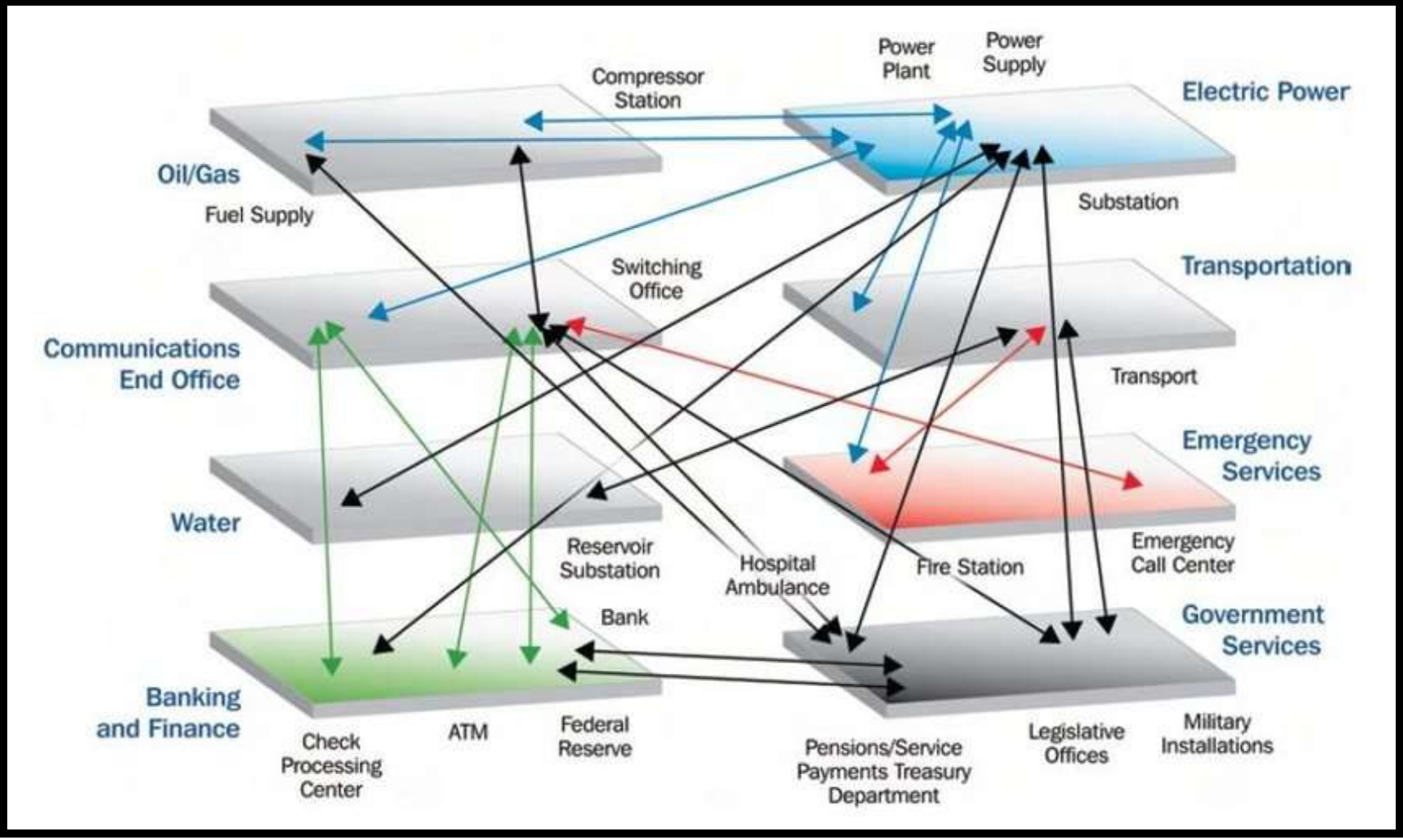
Vulnerable Homelands

A nation's domestic territory and civilian population are exposed to significant risks due to advancements in technology and evolving warfare.

Key innovations

- Water Warfare
- 5th Generation Warfare

Interdependencies between different critical infrastructure sectors

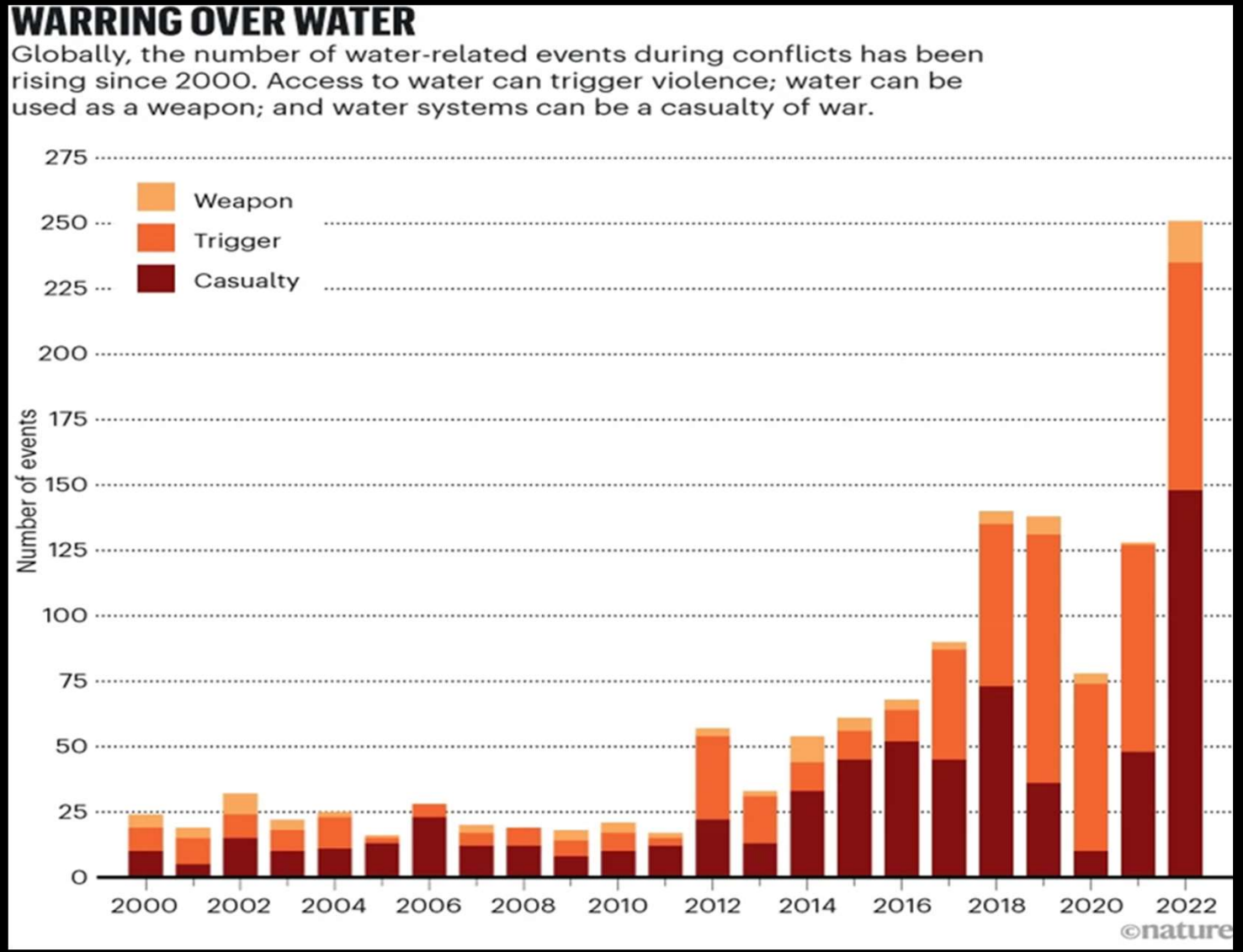


How Hackers Tried to Add Dangerous Lye into a City's Water Supply

A cybersecurity expert explains how safety systems stopped the attack

Iran attempted cyber attack on Israeli water and sewage facilities — report

Fox News says hackers used American servers in last month's attack; Israeli water and cyber officials say attempted breach did not disrupt water supply



"Their Tactics Have Changed: Russia's Bid to Blow Apart Ukraine's Power Grid" - CNN

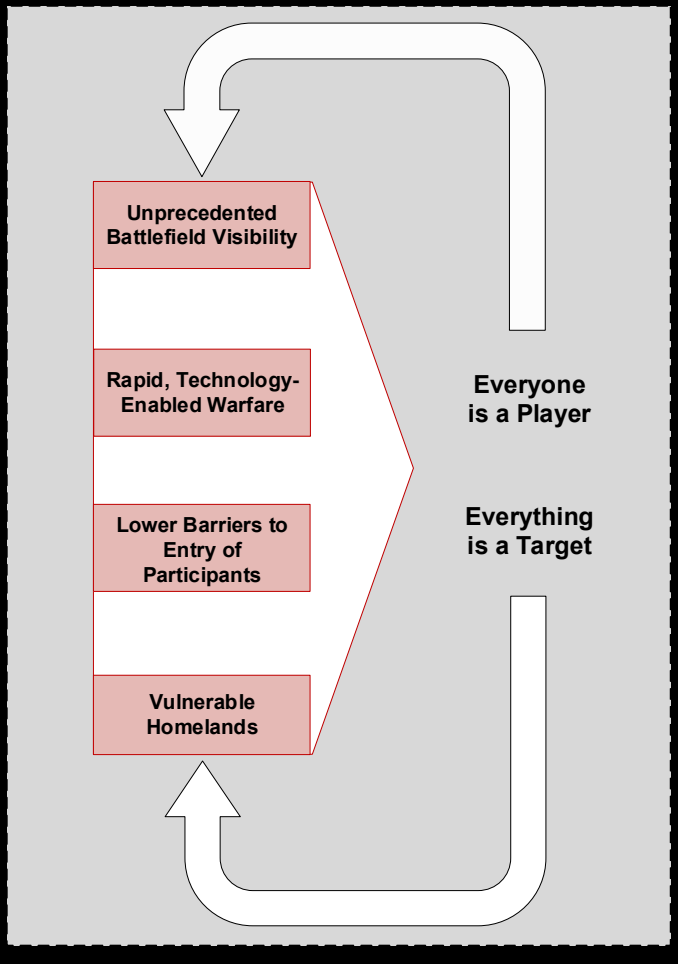
"Russia is particularly focused on improving its ability to **target critical infrastructure**, including underwater cables and industrial control systems, **in the United States as well as in allied and partner countries**, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure **during a crisis**." – Atlantic Council, Sixth Domain

"Banning TikTok Won't Solve the US Social Media Problem" – The Diplomat: Asia, 09APR24

"Fake, Misleading Visuals of Iran's Attack on Israel Spread on X" – NPR, 16APR24

"New Leak of Classified Documents on Social Media Alarms Pentagon" – NYT, 07APR23

Conflict as a Sandbox



An environment with minimally-restrictive application (testing) of new or immature strategies, concepts and capabilities by militaries, the private sector, or citizens thus impacting the trajectory of any conflict.

Driven by

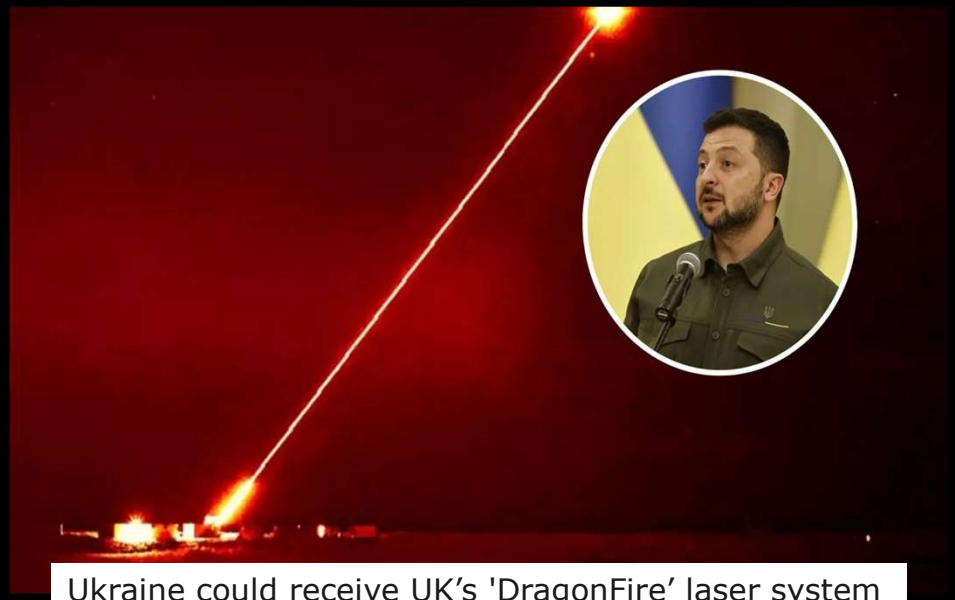
- Continually changing strategies or tactics to confront unprecedented visibility
- Rapid pace of innovation and technology
- Entrance by diverse array of participants
- Increased targets and entry points throughout any homeland

“Army Leaders See Latin America as a test bed for Military Tech” – Army Times

“Businesses Scent a Tech Opportunity in Ukraine War” – Financial Times

“How Ukraine became a testbed for Western weapons and battlefield innovation”- CNN

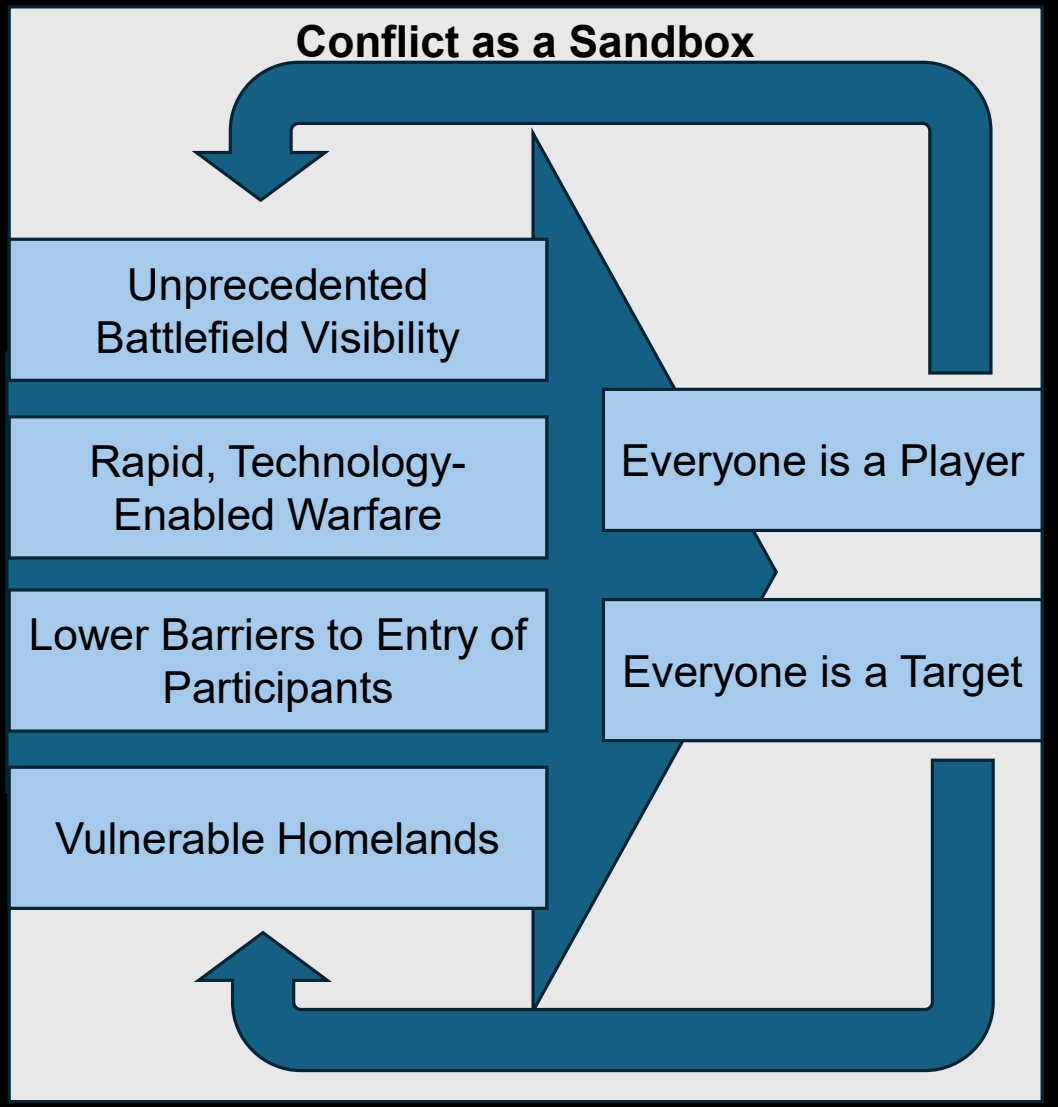
“Shark Tank Kyiv? Investors hunt ‘war-winning’ tech in Ukraine” - DefenseOne



Ukraine could receive UK’s 'DragonFire’ laser system

“How Tech Giants Turned Ukraine Into an AI War Lab” - TIME

How will innovations from contemporary conflicts likely shape the future dynamics of warfare, and what does it mean for Large Scale Combat Operations (LSCO) and pacing threats by 2035?



Thank you!