Still, "smaller" cyber attacks are now happening all the time all over the world—with very serious consequences. Bad actors are asking for larger ransoms and causing more harm. Ransomware is evolving, and future cyber attacks may not be ended by paying a ransom to the cyber criminals.

With many cyber attacks against governments, hospitals and now critical infrastructure like gas pipeline companies and food processing plants taking place, new government actions were a must. These ransomware attacks via different types of malware are becoming more frequent and serious, and are a growing global challenge for public- and private-sector leaders.

Many questions must be answered quickly, such as: Where are the "red lines" that cannot be crossed? Once the lines are identified, what happens if they are crossed? When does a cyber attack become an act of war?

Make no mistake, NATO's new policy on cyber attacks against critical infrastructures is a big deal. Expect more ransomware attacks to occur and those global commitments for action to be tested in the years ahead.

Print Citations

CMS: Lohrmann, Dan. "NATO Adds Cyber Commitments, Potential Ransomware Response." In *The Reference Shelf: National Debate 2022–2023: Emerging Technologies & International Security,* edited by Micah L. Issitt, 25–28. Amenia, NY: Grey House Publishing, 2022.

MLA: Lohrmann, Dan. "NATO Adds Cyber Commitments, Potential Ransomware Response." *The Reference Shelf: National Debate 2022–2023: Emerging Technologies & International Security,* edited by Micah L. Issitt, Grey House Publishing, 2022, pp. 25–28.

APA: Lohrmann, D. (2022). NATO adds cyber commitments, potential ransomware response. In Micah L. Issitt (Ed.), *The reference shelf: National debate 2022–2023: Emerging technologies & international security* (pp. 25–28). Amenia, NY: Grey House Publishing.

result in divergent technological competences that can, in turn, affect the global distribution of power.

Setting Norms—A Role for NATO?

Emerging and Disruptive Technologies (EDTs) came into NATO's political focus in 2019, when NATO leaders adopted an implementation roadmap for seven such technologies. Regardless of their tremendous promise, we must realise that these technologies are not yet mature, not yet "fully out there". Therefore, considerable uncertainty remains to which extent these fledgling technologies and their foreseeable applications are appropriately contained within established legal, ethical, and moral norms. These questions are not limited to military applications, nor do they stop at national borders: rather, they cut across many government departments and business sectors, and they affect humanity in its entirety.

In this complex, fast moving, high-stake setting, we must view technology and values as intertwined. While our values should guide our use of technology, we must recognise that our technology choices will, whether intended or not, reflect the values we adhere to.

As inaction is not an option, we must take active measures to establish norms for the future use of technologies; norms that are deeply rooted in our values; technologies that are currently emerging and have recognised disruption potential (such as AI, biotechnology, and quantum technology). How could we realistically master this novel challenge? The following three proposals could pave the way.

1. We must effectively cope with the uncertainties of technology evolution. Hence, I suggest evolutionary policy-making, building on current knowledge, but flexible enough so that today's decisions can be adjusted or corrected in the future.
2. We must strive to limit potential harm without unduly constraining the benefits a technology can bring. Therefore, our policies should set limits for the application of technologies (such as genetically optimised super-soldiers) rather than banning entire technology areas (in this case, biotechnology).
3. We need to understand when policy changes are necessary and what those changes should be. Reflecting the diversity of interests, we need to institutionalise a broad stakeholder engagement that reaches out to all parties affected by a technology and influencing its evolution.

Within this broadly applicable framing, NATO's role is specific. As the international organisation committed to defence and security in the North Atlantic area, it convenes considerable political, military, economic, and technological power. Building in particular on its political and intellectual capital, the Alliance can credibly spearhead norm setting for technology applications in defence to comply with Western values.

With its recently published AI Strategy, NATO fulfils its traditional role in an innovative way. This Strategy embraces principles of responsible use, which express

Artificial Intelligence in American Culture

Americans have been concerned about the potential for artificial intelligence (AI) for centuries, stretching back to ancient myths of inorganic automata causing havoc among humanity. Many novelists, filmmakers, and other storytellers have used the perceived threat of automated machines that, for one reason or another, turn on humanity. But what about *real* AI? Are autonomous, intelligent systems already a threat to humanity?

Approaching Intelligence

Inspired by ancient myths and science fiction fantasies, scientists have been fascinated by AI for many centuries. The basic idea of AI is to use engineering and mechanical principles to create a system capable of independent and intelligent action. It wasn't until the 1940s and 1950s that scientists began pursuing this goal in earnest by creating the first programs meant to replicate intelligent processes.

Breakthroughs in computer technology between the late 1950s and the mid-1970s allowed for the creation of the first computer programs capable of semi-independent problem solving. This was also the era in which scientists first began developing machines with the capability to comprehend and respond to human speech. At the same time, advancements in optics enabled scientists to begin creating systems to allow machines to "see" visual data, which later led to systems in which machines were programmed to respond to certain visual signals by performing certain actions. Subsequent advancements in computer storage and data management allowed for the creation of "intelligent machines" capable of playing games, like the now famous "Deep Blue," a chess playing computer that was able to compete even with the best masters of the game, or Alpha Go, a machine that was able to beat the best human players in the more complex strategy game known as Go.[1]

In the 2000s, one of the foci in the study of AI was "machine learning," which consists of systems that could gather and retain information and could then use this information to refine decision making. A classic example was the Google Brain experiment of 2012, in which the company created a "computer cluster" that functioned like a brain and then programmed it to teach itself how to recognize a cat after viewing millions of images of cats on YouTube.[2] The capability to learn is a core part of what it means to be intelligent, because a learning system or an individual who can learn also has the capability to improve performance at certain tasks over time.

By the 2010s, this kind of machine intelligence was present in a wide variety of consumer products, and in more advanced forms within machines operated by research organizations and military organizations around the world. In the 2000s, the US military began experimenting with the use of simple AI systems in unmanned the United Nations because a world without it would degenerate into the "Road Warrior." As the late Sen. Daniel Moynihan (D-N.Y.) was fond of saying, everyone is entitled to their own opinions but not their own facts.

Warfare has changed, becoming more Sun Tzu, who valued deception over firepower.

Traditional deterrence no longer works because our adversaries wage war but disguise it as peace. This deliberately confounds deterrence theory, which requires a clear and present danger to trigger the "if/then" logic of deterrence. For example, in the Cuban Missile Crisis, the U.S. told the Soviets that if they deployed nuclear missiles to Cuba, the U.S. was prepared to launch World War III. The USSR backed down—a clear win for strategic deterrence.

Not so today. By disguising war as peace, adversaries bypass deterrence strategy by operating in ways we do not associate with "acts of war." Hence, they can get away with murder, literally. For example, consider whether the following actions rise to the level of war: Cyberattacks and disinformation; China's Belt and Road Initiative (BRI) and debt-trap diplomacy; "gray zone" conflicts and wars "beneath the threshold of war"; China's "lawfare" in the South China Sea; whatever is going on in Libya right now. "Is it war? Is it peace?" asked a military colleague of mine, head cradled in his hands. "If it's war, I know what to do. If peace, that's something else. But it's neither. Or both. What are we supposed to do?"

These "non-war" wars do not bend to the strategic logic of Clausewitz or Thomas Schelling, who prized brute force as the ultimate form of diplomacy (read: "deterrence and war"). Our national security establishment is steeped in these two thinkers. Yet warfare has changed, becoming more Sun Tzu, who valued deception above firepower. You win modern wars not through blitzkrieg, but by manufacturing the fog of war and exploiting it for victory, as our adversaries do. This is strategic deception. Trying to deter it is like trying to win at three-card monte.

War is becoming a strategic scam, and not a contest of brute strength alone. David beats Goliath through trickery, something the U.S. suffered in Vietnam, Iraq and Afghanistan. Yet we have not learned. Deterrence is the reasoning of Goliath, but we are surrounded by Davids. To beat them, we must improve our strategic IQ and think beyond a big "shooting war" that may never occur. Rather, we should ask what is "war" today? It's not our great-grandfather's war. If war is getting sneakier, we must get sneaky with it. We must learn to scam the scammers—after all, Americans are clever people.

Print Citations

CMS: McFate, Sean. "Will Deterrence Work, When Our Foes Wage War Disguised as Peace?" In *The Reference Shelf: National Debate 2022–2023: Emerging Technologies & International Security,* edited by Micah L. Issitt, 132–134. Amenia, NY: Grey House Publishing, 2022.