Technology, Statecraft, and Unrestricted Warfare

Discussion Paper for the Watson Institute for International and Public Affairs

Ambassador Chas W. Freeman, Jr. (USFS Ret.)
Senior Fellow, Watson Institute for International and Public Affairs, Brown University
October 28, 2017, Providence, Rhode Island

Technology is the translation of science into tools. For a long time, people thought that tool use was what distinguishes homo sapiens from other species. It turns out that some other animals also use tools. But, as far as we know, only humans use weapons. More than HOMO HABILIS or SAPIENS, we are HOMO ARMATUS.

Born toothless and clawless, humans arm ourselves to kill others, including our own kind. The ingenuity we display in devising means to murder members of our species defines us as much as our vaunted ability to reason. We devote a great deal of our intellectual capacity to the development of the lethal artifacts and systems that constitute military technology. In the industrialized democracies of the Organization for Economic Cooperation and Development (OECD), about one-fourth of research and development is military. In the United States, this figure rises to one-half or more.

Scientific discovery has brightened, enriched, and extended our lives. It will continue to do so. But the typical human reaction to it is eagerness to apply the technologies it engenders to warfare. We explore how to chip flint, quartz, and obsidian into spearheads, axes, and arrow points not just to hunt animals but also to kill our fellow man. We develop metallurgy to perfect swords, armor, and projectiles. We use chemistry to make not just medicine but gunpowder, high-energy explosives, toxic gases, napalm, white phosphorous, and defoliants.

Humans apply math and physics to understanding ballistics, kinetic energy shock, circular error probabilities, and the measurement of overpressure. We employ insights into the relationship between mass and energy to making nuclear fission and fusion weapons. We use any and all disciplines of physical science to design weapons of mass destruction and the means by which to deliver them.

We reconceptualize cyberspace as a domain like the land, sea, air, and outer space in which to maneuver to surveil, pilfer, subvert, undermine, and attack rivals and their allies. We exploit quantum mechanics to create unbreakable forms of encryption with which to deceive enemies and smoke out their stealthed weapons systems. We look to robotics and artificial intelligence (AI) to enable us to make and deploy autonomous sentries, drones, and other lethal weaponry that kills presumed enemies for us without our having to be there and thus at personal risk.

Analysis of “big data” now identifies individuals and groups for execution by drones. Humans are reportedly already beginning to apply the latest breakthroughs in gene therapy to endowing soldiers with superhuman capabilities. The next step will surely be to pick up where the primitive eugenics of the last century left off and alter embryos to breed a generation of unprecedentedly formidable warriors. Others will bring forth their own super-soldiers to counter them. The dynamic inherent in the "security dilemma" -- in which one side's defensive move is seen by the other as signaling offensive intent -- will ensure that we overcome our scruples and reach for the precision in germ warfare we failed to achieve in World War II. New bioengineering technologies promise to enable us to eliminate people with genotypes we don’t like by creating tailored bacteria or viruses. Why burn villages when you can depopulate them invisibly, anonymously, and once and for all with disease?

In a sense, none of this is new. Technological advances and innovations in warfare in the early twentieth century were so destructive and menacing that our grandparents and great-grandparents took action to limit not just the risk of war but the manner in which combat could legitimately be conducted. They developed the novel concept of an international community. They formulated new laws of war, prohibited the annexation of territory by conquest, banned collective punishment, specified humane treatment for prisoners of war, invented the concept of war crimes, and created transnational institutions to administer the rules on which they had agreed. It worked for a while. But that was in the last century.

Now the erosion of international law, especially the law of war, and the glorifications of amorality that have accompanied the so-called “global war on terror” have removed the constraints from unrestricted warfare. Nations assume they face the worst and prepare to preempt it without regard to the norms embodied in the Nuremberg trials, the UN Charter, and the Geneva Conventions. The opening decades of the twenty-first century have given us a slew of euphemisms for deviations from past standards.

Consider the term, “unlawful enemy combatant,” an off-the-cuff phrase repurposed in 2001 to mean someone who resists invasion or occupation by a foreign military, even if only by “words or speech.” Persons so designated can no longer claim the protections of the Geneva Conventions, demand to know the charges against them, or expect a trial before a regularly constituted court. They may be incarcerated indefinitely while they are subjected to “enhanced interrogation techniques.” (This is a term with an unfortunate pedigree. It is a direct translation into English of the term the Gestapo used to mean torture – *"verschärfte Vernehmung."*) Or murdered outright.

Or think about so-called “targeted killings.” These are extrajudicial executions based on a presumption of guilt assigned by bureaucrats to allegedly dangerous individuals. Sometimes the sole basis for assassination is the religion, physical location, age cohort, or other ascriptive characteristics of these targets. Such slaughter (often carried out by drones) has become the preferred alternative to conventional warfare in aggressive pacification campaigns in West Asia, the Horn of Africa, and the Sahel.

Innocent bystanders killed by sloppy targeting or the misfortune to be near the targets of aerial and special forces attacks are tallied as dead combatants or denied consideration as so much “collateral damage.”

Each of these evasions and euphemisms for what was previously regarded as abhorrent behavior encompasses a violation of traditional canons of morality and precepts of international law. In the aggregate, the mentality they reflect reduces the options of statecraft to menacing, mugging, or murdering those who refuse to surrender to foreign coercion, subjugation, or dispossession. This obviates the need to formulate strategy. It replaces foreign policy with guilt-free homicide. Whatever restraining power the law once had is no more.

This is, in part, because contemporary political thought treats outcomes, not the processes by which they are reached, as legitimizing courses of action. The shift toward considering the ends to justify the means enables technologists to shrug off moral inhibitions as they develop ever more efficient ways of annihilating presumed enemies. There is no reason to expect domestic and foreign “millennials” to be less gifted at moral equivocation than “boomers” have been. What can be done with technology will be done. Some of it will be good. A lot of it will be or should be morally troubling. And much of it will boomerang on its early adopters.

What further technologically-induced changes in statecraft should we now anticipate?   And what might we do to constrain further morally disturbing, destructive uses of science?

Notwithstanding the current U.S. administration's disdain for diplomacy, let me lead off by briefly considering it.

The twentieth century began and ended with iterations of something unimaginatively called "the new diplomacy." This referred to cultural, informational, and political outreach to foreign societies of the sort practiced by China's Confucius Institutes, the Alliance Française, the Goethe Institut, and the late, very-much-lamented United States Information Agency. But it also embraced efforts by governments and civil society to remake the constitutional orders in other nations by supporting and improving the efficacy of domestic agitation for change. Examples include the global movements to ostracize South Africa for apartheid and to boycott, disinvest from, and sanction ("BDS") Israel to end its promotion of illegal Jewish settlements, ethnic cleansing, and ethno-religious discrimination. They also include the democracy-promotion activities of government-organized non-governmental organizations (GONGOs) like the National Endowment for Democracy, a horde of AID contractors and privately financed NGOs promoting various aspects of human rights, and the swarm of American spin doctors that arrived to engineer electoral outcomes in post-Soviet societies as they democratized.

In many countries, the twenty-first century has begun with the banning of most activities of foreign and foreign-supported NGOs. This has been the trend in ethno-religiously restricted partial democracies like Israel, populist authoritarian regimes like Russia, military dictatorships like Egypt, and one-party police states like China. At the same time, the ability to apply AI to big data has created a new class of professional analysts and remote manipulators of social media, news and narratives, attention spans, and political activism at home and abroad. The first uses of this know-how in the United States were for gerrymandering, post-partisan political campaigning, individuated funding solicitations, and the systematic use of social media to induce mass hallucinations and inflame divisions that energize political activism.

If we are to believe the charges against Russia, this once uniquely American bundle of internet-based stratagems has now come home to roost. Americans, too, are allegedly subject to foreign government misdirection of elections through hacking and targeted disinformation campaigns. Whether this actually happened in the 2016 U.S. elections or not, no one has proposed a feasible means by which to prevent big-data-powered manipulative practices from ubiquitously displacing the far more transparent but less potent "new diplomacy." The smoke-filled back room may be out as a determinant of politics. The manipulation of public attitudes and electoral outcomes by ingeniously connected algorithms is in.

This is the golden age of both disinformation operations and surveillance. With knowledge in societies about themselves and the world around them increasingly resident in the cybersphere, the ability of state and non-state actors to shape the opinions of foreign publics is unprecedentedly great. It has never been easier to carry out propaganda and psychological campaigns, political and cultural subversion, or the stimulus of mass disillusion, elite dissidence, and popular anger and despondency in other societies. In times of war, "psyops" can now achieve the rapid dissemination of highly credible spoofed emails, fake news, false reports of embarrassing misconduct on the part of leaders, and other social media reporting that distorts and disrupts situational awareness, policy coordination, and decision-making. Technology is enabling soft conquest by covert action in cyberspace – the erosion of sovereignty by applied science that facilitates subversive measures beyond diplomacy but short of war.

In the face of such trends, some countries, like China, assert that they must isolate their domestic telecommunications and media environment to prevent foreign intrusion into their political processes. Are they necessarily wrong about this? Such self-insulation is deeply offensive to Western values. But what are the alternatives to it as a means of precluding foreign manipulation or disruption of domestic political processes, regime security, and constitutional order? Americans and citizens of other liberal-democratic societies need to do some hard thinking about how best to "secure the blessings of liberty to ourselves and our posterity" in the age of big data, artificial intelligence, and virtual reality.

A brief, further word on conventional diplomacy before I turn to espionage and warfare.

The frequent resort to "summit meetings" between leaders was a twentieth century innovation. In earlier times, such encounters had been rare. This reflected not only the difficulty of travel but also the sense that meetings at the summit carried special risks. As Dean Acheson put it, "when a chief of state or head of government makes a fumble, the goal line is open behind him."

In the twenty-first century, virtual reality technologies and machine translation will allow summits to be staged without the necessity of physical travel or the presence of human interpreters. Almost certainly, there will be a lot more such meetings between leaders. But, if leaders deal directly, without intermediation by those with understanding and empathy for the cultures, languages, and histories of the foreign societies with which they are dealing, will this produce increased concord or conflict? When chiefs of government put their own reputations directly on the line and diplomats no longer fulfill their traditional role as buffers and scapegoats in interactions with foreign states, will compromises become harder? What does social science tell us about how to maximize the chances that virtual summits will aid rather than injure the human capacity for problem solving?

Whether the changes in diplomatic interaction I am forecasting turn out to be good or bad for humanity depends, of course, not just on the quality of the leaders we select and the competence of the staffs that support them, but on how much disorder the collapse of American hegemony and the reemergence of a world of many competing powers produce. Under current circumstances, I cannot say I find this encouraging.

There is an urgent need to rethink what respect for sovereignty means in the age of the internet, whether a rule-bound order can be reconstituted, how to protect domestic tranquility in the face of reduced barriers to ill-willed foreign meddling, and how to influence and conduct the most advantageous relationships with foreign partners and adversaries. These are all very basic questions. In my view, security studies programs like that here at Watson can make a unique contribution by addressing them.

The same is true, despite the secrecy surrounding it, of the impact of technology on espionage. With records maintained in cyberspace rather than in a physical location, a single hack can yield huge insights into allies' and adversaries' understanding of trends and events, their plans for dealing with these, and the character of those among them involved in doing so. Meanwhile, analysis of hacked big data will enable operatives to identify key individual policy actors in foreign polities, exploit their foibles, and facilitate informing, misinforming, or otherwise influencing them directly or indirectly. Operations involving big data provide the perfect means by which to identify potential recruits as spies.

On the other hand, “hard targets” for human intelligence collection (HUMINT) are likely to get even harder to penetrate. Exhibit A is China. The Chinese government’s “social credit system” is to be in place by 2020. This is a proposed nationwide system linking facial recognition software to closed circuit cameras, identity and credit cards, government records, online transaction, internet browsing and digital messaging histories. Managed by AI, it will rate the extent to which individuals and companies in the country live up to standards set by China’s ruling Communist Party for honesty, probity, obedience to laws and regulations, and patriotism (equated to deference to the Party and its directives). High ratings will confer privileges and discounts on services. Low rankings will deprive citizens of these or incur penalties. The system is designed to recognize patterns of individual and collective behavior, sense problematic social phenomena, and recommend appropriate responses by the authorities. Experiments in local versions are already underway in places like Shanghai.

The stated purpose of this AI-enforced exercise in totalitarian social control is a very Confucian focus on the promotion of civic virtue coupled with a philosophy that echoes the Legalism of Han Feizi. The social credit system is supposed to reduce distrust and lawlessness among Chinese citizens, incentivize desirable civic behavior, and facilitate the flowering of a “sharing economy.” It is surely also directed at strengthening internal security. Whatever the merits or demerits of such a regime, you can bet intelligence agencies around the world are concerned about whether or how spies will be able to operate under it. Very likely, where China leads in this arena, other nations will seek to follow.

Meanwhile, if, as history suggests, technological advance is speeded by international tensions, arms races, and wars, we should expect the new world disorder to accelerate it. Some of the changes will clearly be beneficial. Others not so much. Cars may become driverless but so will armored fighting vehicles.

On August 20 of this year, 116 founders of robotics and AI companies from 26 countries, including Elon Musk and Mustafa Suleyman of Google DeepMind, signed an open letter asking the United Nations to “urgently address the challenge of lethal autonomous weapons (often called ‘killer robots’) and ban their use internationally.”

“Lethal autonomous weapons threaten to become the third revolution in warfare,” the letter states. “Once developed, they will permit armed conflict to be fought at a scale greater than ever, and at time scales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways. We do not have long to act. Once this Pandora’s box is opened, it will be hard to close.”

U.N. bans don’t seem to have much effect these days, but we’d better come up with ways of developing and enforcing norms that can regulate this inhuman delegation of warfare to machines. The same is true of the advances in medical science that make it possible to do gene therapy, manipulate embryos to do eugenics, tailor medicines or poisons to individuals or groups, and carry out precision strikes in bacteriological warfare. Unfortunate precedents have already been set by the United States and its security partners in cyber, robotic, and biological warfare. Consider the release of the Stuxnet virus to sabotage physical facilities in Iran, the automated “kill zones” along the borders of the Gaza Strip and the demilitarized zone in Korea, and the tragicomic manner in which Mossad attempted (and failed) to assassinate Khalid Mishaal in 1997.

And ponder the insights of Confucius, Hillel the Elder, Jesus, and Mohammed. There is validity to the “Golden Rule.” What one does to others will eventually be done by them to oneself. Americans are certain to have reason to regret the precedents we have set in our uses of cyber warfare, drones, and high-tech hit teams abroad.

There is no ground for American complacency on these issues. It cannot be assumed that the United States will indefinitely retain the lead in AI, drone warfare, genetic engineering, cyber war, missiles, bomb design, or other technologies. And, if it did, there is little reason to assume that our country, which pioneered the use against our enemies of napalm, nuclear weapons, carpet bombing, and flying robots, would abjure the development and use of new ways to ensure greater lethality for our armed and covert forces.

So, what is to be done?

Technology is morally neutral. As the National Rifle Association (NRA) is fond of reminding us, “guns don’t kill people. People kill people.” One man’s walking stick is indeed another man’s bludgeon. But, linked to diplomacy, weapons can become tools with which to change men’s minds as an alternative to doing them in.

Nothing short of the collapse of civilization can halt the advance of human knowledge. It is how we use science and technology that matters. Clearly, many of the technologies I have mentioned have great potential for good. We must ensure that they are bent to benign purposes. But how can we limit the prospect that they will be used to do evil?

In a world of little faith and great hatreds, religion is unlikely to rise to meet this regulatory imperative. The Trump administration has gone out of its way to declare that it does not accept that there is an international community. It has affirmed that selfish nationalism alone should regulate international behavior. Diplomacy and development are going out of style. Advocacy of arms control wins Nobel prizes but has no traction in a world of intensifying national rivalries.

If there is an answer to how to subdue the technological devils of our violent nature, the only place left to look for it is in social science. By contrast with the physical sciences, social science has so far generated little technology. Now is the time for its practitioners to come forth with applications of what they have learned about human nature and how to modulate it. It is entirely possible that AI-driven analysis of big data will suggest ways to inhibit the worst instincts of human beings and to encourage best practices in diplomacy, intelligence operations, and warfare alike. Given the alternative, it is certainly worth a try.