AN EMERGING THREATS ESSAY

Invisible Threats

by Gabriella Blum

Koret-Taube Task Force on National Security and Law
www.emergingthreatsessays.com

You walk into your shower and find a spider. You are not an arachnologist. You do, however, know that any one of the four following options is possible:

a. The spider is real and harmless.

b. The spider is real and venomous.

c. Your next-door neighbor, who dislikes your noisy dog, has turned her personal surveillance spider (purchased from "Drones 'R Us" for $49.95) loose and is monitoring it on her iPhone from her seat at a sports bar downtown. The pictures of you, undressed, are now being relayed on several screens during the break of an NFL game, to the mirth of the entire neighborhood.

d. Your business competitor has sent his drone assassin spider, which he purchased from a bankrupt military contractor, to take you out. Upon spotting you with its sensors, and before you have any time to weigh your options, the spider shoots an infinitesimal needle into a vein in your left leg and takes a blood sample. As you beat a retreat out of the shower, your blood sample is being run on your competitor's smartphone for a DNA match. The match is made against a DNA sample of you that is already on file at EVER.com (Everything about Everybody), an international DNA database (with access available for $179.99). Once the match is confirmed (a matter of seconds), the assassin spider outruns you with incredible speed into your bedroom, pausing only long enough to dart another needle, this time containing a lethal dose of a synthetically produced, undetectable poison, into your bloodstream. Your assassin, who is on a summer vacation in Provence, then withdraws his spider under the crack of your bedroom door and out of the

---

This essay builds on themes from a joint book project with Benjamin Wittes of the Brookings Institution.

task force on national security and law

HOOVER INSTITUTION
STANFORD UNIVERSITY

house and presses its self-destruct button. No trace of the spider or the poison it carried will ever be found by law enforcement authorities.

This is the future. According to some uncertain estimates, insect-sized drones will become operational by 2030. These drones will be able to not only conduct surveillance, but to act on it with lethal effect. Over time, it is likely that miniaturized weapons platforms will evolve to be able to carry not merely the quantum of lethal material needed to execute individuals, but also weapons of mass destruction sufficient to kill thousands. Political scientist James Fearon has even speculated that at some more distant point in time, individuals will be able to carry something akin to a nuclear device in their pockets.

Assessing the full potential of technology as it expands (and shrinks) requires a scientific expertise beyond my ken. The spider in the shower is merely an inkling of what probably lies in store. But even a cursory glance at ongoing projects tells us that the mind-bending speed at which robotics and nanobotics are developing means that a whole range of weapons is growing smaller, cheaper, and easier to produce, operate, and deploy from great distances. If the mis-en-scene above seems unduly alarmist or too futuristic, consider the following: Drones the size of a cereal box are already widely available, can be controlled by an untrained user with an iPhone, cost roughly $300, and come equipped with cameras.[1] Palm-sized drones are commercially available as toys (such as the Hexbug), although they are not quite insect-sized and their sensory input is limited to primitive perception of light and sound.

True minidrones are still in the developmental stages, but the technology is progressing quickly. The technological challenges seem to be not in making the minidrones fly, but in making them do so for long periods of time while also carrying some payload (surveillance or lethal capacity). The flagship effort in this area appears to be the Micro Autonomous Systems and Technology (MAST) Collaborative Technological Alliance, which is funded by the U.S. Army and led by BAE Systems and U.C. Berkeley, among others. The Alliance's most recent creations are the Octoroach and the BOLT (Bipedal Ornithopter for Locomotion Transitioning). The Octoroach is an extremely small robot with a camera and radio transmitter that can cover up to 100 meters on the ground, and the BOLT is a winged robot designed to increase speed and range on the ground.

Scientists at Cornell University, meanwhile, recently developed a hand-sized drone that uses flapping wings to hover in flight, although its stability is still quite limited and battery weight remains a problem. A highly significant element of the Cornell

effort, however, is that the wing components were made with a 3-D printer. This heralds a not-too-distant future in which a person at home can simply download the design of a drone, print many of the component parts, assemble them with a camera, transmitter, battery, etc., and build themselves a fully functioning, insect-sized surveillance drone.

Crawling minidrones have clearly passed the feasibility threshold and merely await improvements in range and speed to attain utility on the battlefield and viability in the private sector. Swarms of minidrones are also being developed to operate with a unified goal in diffuse command and control structures. Robotics researchers at the University of Pennsylvania recently released a video of what they call "nano quadrotors"—flying mini-helicopter robots that engage in complex movements and pattern formation.

A still more futuristic technology is that of nanobots or nanodrones. The technology for manufacturing microscopic robots has been around for a few years,[2] but recent research has advanced to the point of microscopic robots that can assemble themselves and even perform basic tasks.[3] The robotics industry, both governmental and private, is also exerting great efforts to enhance the autonomous capabilities of robots, that is, to be able to program a robot to perform complex tasks with only a few initial commands and no continuous control. Human testing for a microrobot that can be injected into the eye to perform certain surgical tasks is now on the horizon.[4] Similar developments have been made toward nanobots that will clear blocked arteries and perform other procedures.[5]

Now, situate the robotics technology alongside other technological and scientific advancements—the Internet, telecommunications, and biological engineering—all of which empower individuals to do both good and terrible things to others. From here, it is not hard to conceptualize a world rife with miniature, possibly molecule-sized, means of inflicting harm on others, from great distances and under clandestine conditions. When invisible remote weapons become ubiquitous, neither national boundaries nor the lock on our front door will guarantee us an effective line of defense. As the means to inflict violence from afar become more widely available, both individual threat and individual vulnerability increase to a hitherto unknown degree. When the risk of being detected or held accountable diminishes, inhibitions regarding violence decrease. Whether political or criminal, violence of every kind becomes easier to inflict and harder to prevent or account for. Ultimately, modern technology makes individuals at

once vulnerable and threatening to all other individuals to unprecedented degrees: we are all vulnerable—and all menacing.

In this essay I take on some of the possible ramifications of these technological advances for the potential incidence of violence and its future effects on the existing legal and political order. I first consider the special features of new weapons technologies that, in my mind, are likely to make violence more possible and more attractive; these are proliferation, remoteness, and concealment. All in all, I argue that technology has found a way to create "perfect weapons"—altogether distant, invisible, and untraceable, essentially generating a more leveled playing field among individuals, groups, and states.

I then reflect on the implications of this development for the traditional legal and political categories—national and international, private and public, citizen and alien, war and crime—that still serve as the basis for much of existing regulation of violence, and argue that these juxtapositions are becoming increasingly vague and inapplicable as rationales for regulation of new threats. Finally, I venture to imagine some broader themes of the future defense against the threat of new weapons, both on the international level (a move to global policing) and on the domestic level (privatization of defense). I argue that as threats increasingly ignore conventional boundaries or nationalities and become more individualized, the traditional division of labor between government and citizens and between domestic and international becomes impractical. National defense will require a different mix of unilateralism and international cooperation. Personal defense will have to rely more on diffuse, private, person-to-person mechanisms of protection, as well as concede more power to the government. The very concept of state sovereignty—what it means domestically and what it means externally—would have to be reimagined, given the new strategic environment.

Several preliminary observations are in order. The first is a caveat: To a significant degree, my essay focuses on the technological *threat* side of the equation. It does not envisage the full line of possible complementary defenses. This discrepancy inevitably produces a somewhat myopic picture of the consequences of new technology. Most technological innovations relating to weapons, biology, or the cyber world are closely followed by apprehensions of Armageddon—so much so that in some cases down the ages, there have been preemptive efforts to ban the use of these technologies. Take, for instance, the 1899 treaty to ban balloon air warfare, which is still in force for its signatories (among them the United States). Genetic and biological engineering, which can save and improve lives on a mass scale, have also been met with criticism about

the impropriety of "Man playing God" and predictions of the end of the human race as we know it. And yet the world still stands, despite the existence of destructive capabilities that can blow up Planet Earth hundreds of times over. In fact, some credit the very existence of nuclear weapons and the accompanying nuclear arms race account for a *reduction* in overall violence.

Still, history has proven that offensive capabilities, at least for a space in time, usually outrun defensive capabilities. In the robotic context especially, as costs go down, availability grows and global threat grows with it. Even if defensive technologies catch up with present threats and many of the concerns raised in this essay could be set aside, it is always useful to continue to think about defense as it should evolve vis-à-vis the micro-world in comparison with more traditional modes of defense. Moreover, it is unclear that the case of meeting threats with equal threats—as in the case of nuclear weapons—would yield a similar outcome of mutual deterrence when it comes to personalized weapons of the kind I imagine here. For all these reasons, I find it appropriate, for the purposes of this essay and with the caveat described in mind, to focus on the threat/offense side of the equation.

A second observation is a variation on the first, and has to do with the different roles and functions of technology in general and robots specifically. Like all machines, robots can be put to good or bad use, and the "good" or "bad" often depends on where one stands. On today's battlefields, robots serve a myriad functions, ranging from sweeping for Improvised Explosive Devices (IEDs), to medical evacuation, supply chain management, surveillance, targeting, and more. In this essay, I focus on technology's "life-taking," rather than "life-saving," functions, while keeping in mind that the same systems can be put to use to save victims of atrocities just as easily as they can be deployed for more pernicious purposes.

From among all types of robots available, I focus mostly on robots that are miniaturized, potentially invisible, which make detection and accountability a great deal more difficult. This is what also situates the "spiders" within the broader technological developments of the Internet, bioengineering, and the like, which, together, constitute an environment in which the threat is largely invisible. Again, although their full scientific and operational potential is unknown as of yet, I assume that some version of miniaturized drones—whether independently operated or deployed off of larger structures that carry them to their target—is a real possibility.

Technology and the Incidence of Violence

Socialization has always been essential for survival. The Internet, media, telecommunications, travel, and commerce have all made the world smaller and strengthened global interconnectedness and socialization. In his recent eloquent and wide-ranging book,[6] Harvard psychologist Steven Pinker argues that our present society is the least violent in recorded history, in part, because technology, trade, and globalization have made us more reasoned, and in turn, more averse to violence. Notwithstanding Pinker's powerful account, the very same technology that brings people closer—computers, telecommunications, robotics, biological engineering, and so on—now also threatens to enable people to do each other infinitely greater harm than of old.

Whether advanced technology really threatens single-handedly to reverse our trajectory toward a less violent world is impossible to predict, precisely because the threat that derives from technological advances is only one manifestation of a sea-change in social and cultural relations which technology as a whole brings about.

Put differently, threats derive from the combination of capabilities and motivations to engage in harmful activities. Technology influences both capabilities and motivations, but not in a single trajectory; the technology to inflict harm is countered by the technology to prevent or correct against it, and motivations to inflict harm are constantly shaped and reshaped by the local and global environment. Any assessment of the future level of threat brought about by new weapons technologies must thus engage with predictions about the growth of capabilities to inflict violence on the one hand, and the growth of or decline in motivations to inflict violent harm, on the other.

As I earlier noted, I am focusing here on the capabilities to inflict harm and their effects on the possible motivations to harm, but only in the narrow context in which some underlying motivation to injure others exists. Of course, if political, ideological, or personal motivations for harm are significantly reduced, for instance, because interconnectivity and interdependence diminish violent hatred, demonization of others, or the attractiveness of violence as means of promoting ideological goals, we have less to worry about.

With all their uncertainties, however, it seems to me that the lethal capabilities of miniaturized technologies will spread well before what has been assumed to be pacifying social forces, whether the Internet or reason, will have operated to turn much more of our world into a peaceful place. Even if they do not, considering those

features of new weapons technologies that enhance the capability—and perhaps, therefore, the motivation—for violence warrant special attention.

Violence, of course, does not require fancy weapons. Even in our present age, it took mostly machetes for Hutus to kill 800,000 Tutsis and moderate Hutus in the course of only 100 days. Individuals everywhere are already vulnerable to the proliferation of weapons. According to some estimates, there are 90 guns for every 100 people in the United States, and more than 800 million firearms worldwide. Between 10,000 and 20,000 people are killed annually in gun-related homicides in the United States. These homicides account for two-thirds of all murder cases. When people want to kill other people, they can.

And yet, three features of new weapons technology—proliferation, remoteness, and concealment—make violence more likely. All three are already present to some degree in existing weapons, but new technology integrates and intensifies them in a way that significantly enhances their potential threat. In what follows I discuss these three features in greater detail.

While my focus is on the microdrones or other "invisible" robots, I allude in this discussion to other robotic technology. This is both because the full potential of such invisible weapons is still uncertain, and because it is easier to demonstrate the features under consideration vis-à-vis familiar existing platforms. Miniaturization is just the next step that would make threatening features that much more pronounced.

Proliferation

While many kinetic weapons are relatively cheap and easy to make, the weapons that allow for long-range strikes—airplanes, missiles, and the like—are neither cheap nor easily obtainable, and are therefore limited to developed states' arsenals. Developing states and non-state armed groups often have access only to mortar rounds, anti-aircraft, anti-tank, and other short- and medium-range rockets. Few armed groups have access to longer-range munitions, and none that I know of has its own aircraft. True, it is already possible to fly an airplane into a building; but it is hard to do it repeatedly, especially from outside the state's boundaries.

Forty-five countries presently rely on robots of various sorts, and these numbers will only increase. My working assumption is that robotic technology will proliferate until it becomes pretty much available to everyone in whatever color of market. This is not true for all weapons technologies, but several considerations make it more likely in

this context: First, much of the development of robotic technology occurs not in the governmental sector but through public-private partnership. iRobot, a Medford, MA, company that makes the Rumba (a robot vacuum-cleaner) also makes drones for the U.S. military. The iDrone operating program in particular shows the permeability of defense development by the commercial market. While the program was developed by the Massachusetts Institute of Technology in conjunction with Boeing for military application, it became widely available within months of its successful completion. While hardware continues to take longer to make the transition from military to civilian application, the availability of Parrot AR and other commercially available surveillance drones makes it clear that the lag is one of degree of capability rather than one of kind.

Second, the pace of manufacturing and deployment of robots has been very rapid. In Afghanistan and Iraq, around 20,000 robots are now deployed, more than a hundred times their original deployment 10 years ago. In recognition of the certain proliferation of drones, in both the governmental and private sectors, the Federal Aviation Authority was recently directed by Congress to develop a plan to integrate Unmanned Aerial Vehicles into U.S. airspace by 2015.

Third, at least the basic technology and operation of drones is not overly complex. DIYdrones.com already informs people how to build their own personal drones. The website does not instruct its visitors on how to arm these drones, but such instructions eventually tend to find their way onto the Internet, just as instructions on how to build IEDs have. In short, you can already build your own surveillance drone for your personal use. Arming it is just the next step.

As robots and drones become cheaper, simpler to make and operate, as well as more autonomous and more widely available, there is every reason to suspect that additional countries, armed groups, and indeed individuals will be among their best patrons. In fact, the Lebanese armed group, Hezbollah, has already made use of drones (delivered to the organization from Iran). And, more recently, in September 2011, a 26-year-old Massachusetts man with a degree in Physics has been charged with plotting to fly explosives-filled, GPS-guided drones into the Pentagon and U.S. Capitol.[7] Moreover, if "spiders" can one day be armed with WMDs, James Fearon's image of people carrying small nuclear bombs in their pocket becomes more than a figment of his imagination.

The proliferation of weapons brings about a democratization of threat, which is a real cause for concern. Countries can generally be monitored, deterred, and bargained

with. Individuals and small groups are much harder to police, especially on a global scale. Effective state structures, as Pinker points out, have played a crucial role in maintaining law and order and curbing violence within the state. Today, of 194 states, 35 appear on the U.S. Fund for Peace Index of failed or fragile states on high alert. The coupling of empowering technology and weakened state structure exacerbates the risk of nonstate violence both within and from the state's territory.

Protecting governmental monopoly over explosives, guns, or computer technologies has been a near-impossible task. Securing one over deadly drones and minidrones in the future will likely prove even less successful, especially given the possibility of "homemade" drones. As weapons become smaller and easier to make, regulating their manufacture and trade becomes an impossible task. As with cyber threats, developers and producers are increasingly capable of concealing the origin of a device; and as the number of potential sources (in addition to individual manufacturing) increases, secrecy and deniability become endemic to the industry.

There is reason to believe that the empowerment of individuals in new and expanded ways will affect their motivations to act. In the political-ideological violence context, the easy availability of spider technology would enable individuals everywhere to take violent political or ideological action against targets that they would not otherwise have easy access to. They might take violent action to promote their own agenda, or even to promote a national agenda, but through private means. Consider an analogy from the cyber world: "Patriotic hackers" is the name given to private individuals who sympathize with a government's hostile position toward others and engage in privately undertaken cyber attacks against those whom the government perceives as its enemies. Now imagine the patriotic spiderman—the individual who privately deploys destructive capabilities against the state's proclaimed enemies.

Proliferation of spider technology might ultimately affect not only the levels of political violence, but also private, inter-personal violence as well. It is already easy enough to kill a fellow human being. Having simpler means with which to do so might tip the scale, however, from contemplation to action. I return to this point in the following sections.

On the flip side, one could well raise the question why proliferation has not affected the incidence of attacks by biological or chemical weapons. Although many states take significant measures to combat the proliferation of these types of weapons, public commentary is rife with reports on the ease and simplicity with which dangerous materials are available for harmful use; and yet, to date, we have seen very few

unconventional attacks worldwide. I do not have a good answer to this (happy) conundrum. Still, my prediction is that drone technology will become far more ubiquitous in the foreseeable future than chemical or biological weapons, thereby affecting not only the availability of robotic weapons but also the psychological and social aversion to their deployment. The possibility that such platforms would ultimately be armed with unconventional weapons must be seriously considered, even if its probability can be debated.

Remoteness

We are already vulnerable to remote strikes, whether they originate from within the state or from outside of it and whether they are delivered by states or by nonstate actors. In fact, from the moment people stopped fighting with fists or clubs and began to rely on spears, catapults, crossbows, and gunpowder, the overriding focus of warring parties has been to increase their distance from their enemies, to strike the enemy from as far as possible while protecting themselves from counterattacks. Mortar rounds, rockets, and a range of other kinetic weapons allow for attacks from outside a country's borders. The advent of air warfare and the development of long-range air-to-surface and surface-to-surface missiles already make states, groups, and individuals vulnerable to attacks originating from thousands of miles away. Considered in this light, the F-16 aircraft and the Tomahawk guided missile are no more than a continuation of the crossbow—and the Predator drone is a mere continuation of the F-16.

Robots do make a difference, however, in at least three ways. First, and related to their proliferation, they provide more actors with more capabilities of striking from afar, potentially, on a mass scale. Without the need for complex organizational, scientific, and financial structures that are necessary for ordinary long-range weapons, eventually every citizen will become empowered to strike at targets situated hundreds and thousands of miles away on a repeated basis. Of course, the smaller the targeting device is, the harder it is to deploy it from great distances (birds can fly across oceans, insects generally cannot), but it is possible to mount very small devices on a larger device and transport the latter over great distances.

A second implication of remoteness is that with the growing ability to project power from afar, without risking too many human lives or expending too many resources, domestic political barriers to extraterritorial violence might further diminish. Again, robots in this sense are only an extension of the Tomahawk missiles or air power more generally. The 1999 war in Serbia, for example, was conducted with no boots on the

ground, and the NATO operation in Libya was defended as constitutional by the U.S. administration, even though it was not approved through the War Powers Resolution process, in part because U.S. military personnel did not set foot on Libyan soil. But as robots increasingly allow for "no boots on the ground" operations, cheaper and simpler from reliance on manned air vehicles, the incidence of robotic extraterritorial violence may be higher, for better or for worse, than the incidence of traditional forms of extraterritorial wars.

Any hope that a level playing field would ultimately result in robots fighting one another, rather than in robots fighting humans, is likely to be a false one. If a war between robots, whether miniaturized spiders or the large Reaper drones, were possible, all wars could be resolved through video games or duels. But wars are ultimately fought between humans and need to hurt humans to matter. The fewer humans available to hurt on the battlefield, the more humans outside the battlefield will pay the many pounds of flesh to suffering and death that are required by war.

At the same time, for actors committed to humanitarian ideals, the coupling of remoteness and precision allows for the possibility of striking only those most "deserving" players—political leaders, military commanders, and the like. In this aspect, robotic technology could prove "life-saving" not only on the part of the targeting country, but on the part of the targeted country as well. In fact, there is a strong argument to be made that notwithstanding the current laws of war, with individualized-precise targeting methods, and without any risk to the targeting forces, foreseen "proportionate collateral damage" should be zero, absent special justifications.

A third, violence-exacerbating feature of remoteness is that it creates a mental distance between the attacker and his victim. When the body is out of harm's way but one's mind is engaged in a play-like environment of control panels and targets moving onscreen, killing can quickly turn into a game. There is much debate over whether drone operators in the U.S. military actually develop a numbing "play-station mentality"[8] or, to the contrary, suffer from higher levels of post-traumatic stress disorder compared with their comrades on the physical battlefield.[9]

In any case, even if the numbing effect of remoteness can be countered by training, monitoring, and intervention, such responses are relevant to militaries or other organized structures, but less so to private or diffuse individuals. Numbing is thus potentially more dangerous in the context of "ordinary" criminal violence: Although

people rarely have an interest in killing random people unless they are insane or sadistic, remoteness from a victim, greater than that enabled by a simple handgun, is likely to weaken human inhibitions regarding harming others. In fact, it is likely that at least part of the inhibition to harm others derives exactly from seeing, hearing, and feeling one's victim in the vicinity of our own bodies. Blinded killing might be a little less unattractive.

Concealment

In Plato's *The Republic*, Glaucon and Socrates disagree on what makes people behave justly or virtuously. In support of his claim that people act morally only when they fear punishment for bad conduct, Glaucon offers the tale of Gyges of Lydia, a shepherd in the service of King Candaules. Finding a golden ring that enables its wearer to become invisible, Gyges arrives at the palace and under his new power of invisibility, seduces the queen, murders the king, and takes his place on the throne.[10]

At present, much of our political, strategic, and legal frameworks for dealing with violence assume that the violent act can be attributed to its source and that this source can be held accountable—through a court of law or retaliatory strikes. In many cases, the perpetrators of violence have no desire to mask their responsibility; it is not infrequent that more than one organization claims responsibility for a terrorist attack in a bid for credit and recognition.

But to those who do wish to conceal their involvement, microrobots, like cyber attacks, offer invisibility. Being near-impossible to regulate, monitor, or detect, they empower perpetrators not only to strike with impunity, but in some cases, to cover up the very occurrence of the attack. Absent the ability to attribute an attack to its source, human violence becomes no different from natural disasters—a harmful event for which the only effective remedy is preparedness, recovery, and prayer.

Of course, even at present, not all violence is detected or prosecuted and enforcement in some jurisdictions is lacking. Some people do get away with murder, and states are often successful in operating in a clandestine manner, leaving no trace behind. And yet, detection and accountability make considerable disincentives for both political and criminal violence (the assassination by the Israeli Mossad of Hamas leader Mahmoud al-Mabhouh in Dubai was caught on tape almost from beginning to end, probably affecting the planning and execution of future operations of this sort). Perpetrators of violence are aware of the fact that the same technologies that make all of us naked and vulnerable—namely, monitoring, surveillance, and forensic science—

all make violence more difficult to conceal. If defense systems evolve at the same pace as microdrones, spiders will not necessarily prove any more threatening than handguns. If, however, violent technology outpaces mechanisms for defense, detection, and accountability, a free pass for killing will become widely available.

While concealment holds obvious attraction for covert military action, one might doubt the attraction of a free pass for murder for the ordinary person. If we believe, as Plato did, that the possibility of getting away with murder does lower the inhibition to commit it, then the prospect of spider drones is an apocalyptic vision. Indeed, some contemporary studies suggest that the fear of getting caught is a greater deterrence for would-be perpetrators than any punishment offers.[11] Moral inhibitions need not operate similarly for everyone: In a world of 7 billion people, 1 percent is 70 million people.

Breaking Down Categories

The advent of transnational terrorism in recent decades has already been associated with the breakdown of traditional categories around which much of our legal and political architecture is designed. These categories are often organized as dichotomies: public vs. private, domestic vs. international, territorial vs. extraterritorial, citizens and aliens, war and crime. As new technologies empower individuals everywhere to strike individuals everywhere, the applicability of these juxtaposed categories, as well as their conceptual justification, will be further eroded.

The democratization of threat makes it harder to connect attacks to their sources. Without such ability, no retaliatory, punitive, or even preventive action can be taken effectively, and must result in affecting too few potential perpetrators and too many innocent people. The problem is further exacerbated when individuals act not only on their own behalf, but for some broader ideological or national goal: in those cases attribution becomes problematic not only at the level of connecting a particular attack to a particular individual, but also in connecting a source of attack to a broader organizational structure. Without the ability to attribute the attack, the concept of state (or other organizational) responsibility as we currently know it disappears, and with it, the distinction between public and private action.

If new technologies now enable anyone to strike just as easily from outside the borders of the state as from within them, state boundaries can no longer serve as good conceptual or practical lines of defense. For the same reasons, nationality is no longer a good marker for either friend or foe. Consequently, the interests of states in

exercising their jurisdiction over individuals can no longer follow the current division between domestic jurisdiction (where states have full legislative, adjudication, and enforcement powers) and international jurisdiction (where a justification—tied to a particular type of person or activity—is required to allow the state to exercise its powers outside its boundaries). Both territory and nationality become less persuasive as grounds for dividing up the powers of regulation and enforcement.

The empowerment of individuals further contributes to the collapse of the crime/war distinction. Traditionally, what had distinguished one form of violence from the other were the nature of the perpetrator of the violence (private individual vs. government or organized armed group), the motivation behind the act (private interest vs. ideological), and the scale and effect of violent action. Like guns and cyber attacks, spider drones can be used by both criminal and politically motivated enemies, by individuals as well as collectives, and on a small or large scale. Just like the debate over the classification of terrorists, who are criminals for some purposes and combatants for others, we should anticipate much debate over the treatment of individuals who engage in spider attacks. Coupled with the diminishing significance of either territory or nationality as grounds for regulation, the distinguishing significance of the motivation for violence seems to diminish as well. "Threat" and "guilt" thus become intertwined, both on the national and individual levels.

All this means that we must work to conceptualize a framework for dealing with transnational violence (that would include terrorists, pirates, transnational criminal networks, etc.), which does not fall neatly within the category of crime or category of war, which takes into account boundaries and nationality for some purposes but not others, and that reconceptualizes what sovereignty means in the twenty-first century, both domestically and internationally.

What Does Defense Look Like?—Sovereignty Reimagined

As the previous section argues, a transnational model for the regulation of violence must take on both a policing and a warring mode. These should include a mixture of monitoring and detection, prevention, deterrence, retaliation, and incapacitation. The complex strategy must be geared toward individuals as well as groups or states; and since the battlefield is potentially everywhere, these modes of response cannot be confined to the national territory, but must be imagined on a global scale.

Global policing (a term I use here to denote this model of transnational regulation of violence) is a much more complex task than either conventional domestic policing or

traditional wars. Essentially, it requires defending every individual against all other individuals—citizens or foreigners—a much harder task than defending a state against all other states or individuals against their fellow citizens. Meeting this challenge would require a renegotiation of both the international and national orders.

On the international level, in a world of policing in which territorial boundaries and nationalities are of faded relevance, there will be growing pressures in two opposite directions: One toward greater international cooperation, the second toward unilateral action.

As for international cooperation, with no state capable of singlehandedly policing all individuals around the world, interstate cooperation in detection, prevention, and punishment of perpetrators of violence must become even more vital than it is today. Cooperation could take many different forms, ranging from harmonization of regulation, through exchanges of information and intelligence sharing, to a multinational policing force with powers of enforcement.

An opposite trajectory, however, will be toward greater unilateral action, especially in cases in which the territorial state proves incapable of or uninterested in policing its own people effectively. The "unable or unwilling" test for breaching state sovereignty without the local state's consent—contested as it currently is in the context of targeted killing operations—will continue to be debated, negotiated, and shaped by those most able to project force outside their borders. We will have to reconsider the rules on state responsibility and decide on the right standard of attribution, or in other words, on what states owe each other in terms of protecting other states from threats emanating from their own territory. The reformulation of state sovereignty as responsibility would have to consider not only the responsibility of states toward their own citizens, but also the responsibility of states to harmful externalities that emanate from their territories and injure other states and their citizens. At the same time, sovereignty-as-responsibility cannot be limited to negative duties of harm avoidance; we must also reconsider what states owe each other in terms of affirmative duties of assistance in state-building. It is now in the developed world countries' clear interest, if not their moral duty, to ensure that there are fewer fragile or failed states around the world, and that states have a real capacity to police their territory in an effective way.

New technologies are likely to affect not only the international order, but the domestic one as well. The organizing principle of the traditional social contract has been that the sovereign protects its citizens from the Hobbesian state of nature—anarchic

violence among individuals—in exchange for securing its own monopoly over the use of force. Under this contract, only the police or dedicated governmental authorities may exercise force against citizens within the state and against foreign enemies threatening the state from the outside. In exchange, citizens are expected to bow to the law of the state and stand ready to defend the state from external threats.

This social contract can endure only for as long as the government is in fact effective in maintaining law and order and in protecting its citizens from both external and internal threats. If new technology laughs in the face of policing, and if the proliferation of lethal power triumphs over anything the state can do to protect its citizens, the contract loses its hold. In the era of "the democratization of weapons," as the NRA calls it, democracy stands a good chance of sliding very quickly into anarchy. The more weapons we amass as individuals, the more we abdicate the power of the state to protect us.

Earlier rumors about the death of sovereignty have all turned out to be premature. As Philip Bobbitt has convincingly demonstrated, the market state replaced the nation state by adapting to changes in financial and commercial markets, rather than dissipating altogether.[12] In the same vein, states need not be rendered powerless vis-à-vis the new technologies: A state can regulate, monitor, and report the proliferation and use of lethal technologies. It can develop defensive technology and a defensive, technological army. It can deploy its resources to monitor, track, and punish violent offenders (police forces in the United States are already using surveillance drones).

So far, however, history proves that regulation of offensive capabilities is only partially effective, and that technology often outpaces governmental regulation. As Joel Brenner has observed in the context of the cyber world, "law is chasing reality, not shaping it."[13] Monitoring and accountability will account for some, but not all, acts of violence, and overall, might well prove less effective than in the case of ordinary weapons.

To achieve better monitoring and meet violent threats, domestic and international, there will be need for a harsh tradeoff: The state will have to increase its powers of surveillance of individuals, preemption and prevention, at the cost of traditional perceptions of privacy and liberty. Indeed, our most intimate notions of what privacy and liberty look like will have to be reimagined and adapted to a world in which we are all constantly naked and vulnerable. If, traditionally, we imagined privacy and liberty as having to be guarded from the incursion of the Leviathan of government power, it is now our fellow citizens (of our own nation or the world) whom we should be

concerned about, as we call on the Leviathan to exercise even greater power than heretofore at our own expense. The democratization of threat thus threatens our conventional notions of democracy.

In parallel, as the state becomes less dependable for providing safety, citizens everywhere will have to find their own modes of protection. One, like alarm systems or personal handguns, will be purchased on the open market, and market forces will supply the need for defense and regulation of weapons. Another, like vigilantism or community policing, will take the form of people-to-people networks of monitoring, preemption, or even punishment of offenders. These networks will not be confined to national borders, just as professional communities of hackers are not confined to any one state. One recent example of this trend has surfaced around a new iPhone app that is designed to track stolen phones: The phone can be programmed to photograph its holder, thereby taking a photo of anyone who steals the iPhone from its rightful owner. Pictures of alleged iPhone thieves are posted on Facebook as "Wanted" billboards used to be in the Wild West, with owners inquiring whether anyone recognizes the thief in the picture. The iPhone case assumes, of course, the ability to attribute the theft to a particular person, but it nonetheless demonstrates how individuals are becoming reliant on social networks for restoring their property (and also of how technology can be developed to protect itself from being misused). One could imagine further development of this idea to the realm of new weapons.

▪ ▪ ▪

A final note on threat perception: Micro and invisible weapons are undoubtedly scary. While we are all constantly vulnerable to natural disasters, disease, human violence, and accidents, the empowerment of individuals everywhere to harm us at any given moment, without much risk or accountability, seems a nightmare at the present moment. If it comes, it may drive us all to remain in secure quarters, associate only with those we know and trust, and engage as little as possible with the outside world. Thus, globalization will grow across one vector, only to be met with a counter-vector of tribalism and kinship.

But human experience has always involved learning and adaptation. Though it is almost two centuries since mankind has discovered bacteria, also an invisible enemy, as well as an invisible friend, it was learning about the threat (which has always been around) that has taught us how to deal with it. We clean, we sterilize, we vaccinate,

we guard laboratories against biological theft, we eat "good bacteria" for our stomachs.

As with any new danger, manufactured or discovered, we learn to live and cope with threats, to normalize the abnormal. There is no other way to deal with the constant dangers that we already face. The world, and those who inhabit it, will have to adapt to new technologies just as it has to all previous technology. After all, as one psychiatrist friend pointed out to me, "invisible threats" are the very definition of paranoia.

Acknowledgments

I thank the participants of the National Security and Law Task Force at the Hoover Institution, as well as Nathaniel Laor and Andrew McAfee, for their comments and engagement. I am also indebted to Lucas Issacharoff, Brian Itami, and Sonia McNeil for their excellent research assistance.

Notes

1 See, e.g., the iDrone or the Parrot AR Drone.

2 Brian Handwerk, "New Microscopic Robot's Tiny Step Is a Huge Leap," *National Geographic News*, October 6, 2005, http://news.nationalgeographic.com/news/2005/10/1026_051026_tiny_robot.html.

3 Henry Kenyon, "Energy lab's microscopic robots assemble selves, can move larger objects," *Government Computer News*, August 30, 2011, http://gcn.com/articles/2011/08/30/argonne-lab-microscopic-robots.aspx.

4 Olivia Solon, "How to drive a microscopic robot around the inside of your eye," *Wired.co.UK*, April 27, 2011, http://www.wired.co.uk/news/archive/2011-04/27/eye-robot.

5 See, e.g., NanoDocs at RYT Hospital page, accessed May 28, 2012, http://www.rythospital.com/nanodocs.

6 Steven Pinker, *The Better Angels of our Nature* (2011).

7 Milton J. Valencia and Brian R. Ballou, Rezwan Ferdaus indicted for alleged plot to attack Capitol, Pentagon, *The Boston Globe*, September 29, 2011. Available at http://www.boston.com/Boston/metrodesk/2011/09/alleged-terror-plotter-indicted-federal-grand-jury/OevOhHc4o1VwcQABMplHIN/index.html

8 Philip Alston and Hina Shamsi, "A Killer above the law," *The Guardian*, August 2, 2010, available at http://www.guardian.co.uk/commentisfree/2010/feb/08/afghanistan-drones-defence-killing.

9 Elisabeth Bumiller, "Air Force Drone Operators Report High Levels of Stress," Elisabeth Bumiller, *The New York Times*, December 19, 2011, available at http://www.nytimes.com/2011/12/19/world/asia/air-force-drone-operators-show-high-levels-of-stress.html

10 I am grateful to Peter Berkowitz for referring me to this parable.

11 John Braithwaite and Toni Makkai, Testing an Expected Utility Model of Corporate Deterrence, 25 *Law & Soc'y Rev.* 7, 8 (1991) (citing studies finding certainty of sanction is more reliable deterrence than severity); Paul H. Robinson and John M. Darley, Does Criminal Law Deter? A Behavioral Science Investigation, 24 *Oxford J. Legal Stud.* 173, 183–193 (2004).

12 Philip Bobbitt, "The Shield of Achilles" (2002). See also Stephen Krasner, who argues that state sovereignty was never as sacrosanct as it is believed to have been, and that it is only our perceptions of legitimate types of intervention in other states' sovereignty that have changed; Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (1999).

13 Joel Brenner, America the Vulnerable, at 23.

The preferred citation for this publication is
Gabriella Blum, "Invisible Threats (2012)," in *Emerging Threats in National Security and Law*, edited by Peter Berkowitz, http://www.emergingthreatsessays.com.

About the Author

Gabriella Blum
Gabriella Blum is the Rita E. Hauser Professor of Human Rights and International Humanitarian Law at Harvard Law School (HLS) and the codirector of the HLS-Brookings Project on Law and Security. Previously, she was a senior legal adviser in the Israel Defense Forces and a strategic adviser in the Israeli National Security Council. She is the author of Islands of Agreement: Managing Enduring Armed Rivalries *(Harvard University Press, 2007) and* Laws, Outlaws, and Terrorists: Lessons from the War on Terrorism *(with Philip Heymann) (MIT Press, 2010).*

Koret-Taube Task Force on National Security and Law

The National Security and Law Task Force examines the rule of law, the laws of war, and American constitutional law with a view to making proposals that strike an optimal balance between individual freedom and the vigorous defense of the nation against terrorists both abroad and at home. The task force's focus is the rule of law and its role in Western civilization, as well as the roles of international law and organizations, the laws of war, and U.S. criminal law. Those goals will be accomplished by systematically studying the constellation of issues—social, economic, and political—on which striking a balance depends.

The core membership of this task force includes Kenneth Anderson, Peter Berkowitz (chair), Philip Bobbitt, Jack Goldsmith, Stephen D. Krasner, Jessica Stern, Matthew Waxman, Ruth Wedgwood, Benjamin Wittes, and Amy B. Zegart.

For more information about this Hoover Institution Task Force, please visit us online at www.hoover.org/taskforces/national-security.

HOOVER INSTITUTION
STANFORD UNIVERSITY