Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

le

e CIA Can't Hack Senate Computers cause They Own Them, Experts Say

STERNSTEIN

ing Outcomes

ing this article, you will be able to:

the Computer Fraud and Abuse Act as the closest
erica has to an anti-hacking law.

ifficulty in defining access entitlement based on
p of the Senate computers.

n debate over appropriate (if any) disciplinary
s for the CIA IT employees.

personnel probably didn't commit a hacking crime
rummaging through congressional computers used
research the agency's torture activities, former fed-
ys and scholars say.

wmakers are calling for a criminal probe into new
a CIA inspector general that the agency improperly
enate intelligence committee files about its detention
gation program. Committee staff has been compil-
condemning the program.

an agreement, only CIA information technology
were allowed to access the system, says commit-
oman Sen. Dianne Feinstein, D-Calif. The CIA
t agreement by removing about 920 agency items
ing through the committee's own internal work, she

CIA provided the system, network drive, search tool,
ed documents.

ing data from that network, if it's your network,
's difficult to make it hacking," said Ben FitzGerald,
f the Technology and National Security Program at
for a New American Security.

ds to be careful with the term "hacking," he said.

Not Much Legal Ground to Stand On

The argument that the CIA violated the closest thing America has to an anti-hacking law—the Computer Fraud and Abuse Act—likely won't carry much weight in court, say former U.S. attorneys. This is because the law is mushy when it comes to who is a computer's rightful operator. And there are intelligence-collection loopholes that could clear the CIA. Also, the agency could argue there was no deliberate effort to inappropriately penetrate the system.

"You have to knowingly access a computer without authorization" to break the law, said Mark Rasch, former head of Justice's Computer Crime Unit. CIA officials probably will claim that "while they did access the computer, they didn't know that they didn't have authorization to do it," as the actions were approved by agency superiors.

The legislation also makes an exception for "lawfully authorized" investigative, protective, or intelligence activities, he noted.

A teenager, however, who tried this stunt probably would be paying fines or would be confined to a prison cell.

"Ordinarily, if I was not a CIA employee and I broke into a computer to get classified information, that would be like espionage and be a serious criminal offense," said Rasch, now a private consultant.

Sen. Ron Wyden, D-Ore., on Friday morning told MSNBC's Chuck Todd: "If a 19-year-old hacker had searched Senate files this way, that hacker would be sitting in jail right now. Now, back in January, I asked [CIA Director John] Brennan whether the Computer Fraud and Abuse Act applied to the CIA. That act has criminal penalties . . . I want to know who is going to legally held responsible."

Other former federal attorneys say it's unclear who held access rights to the system and the law hinges on that detail.

"Who has the superior claim to control access? I don't think there's an obvious answer," Orin Kerr, a former official with Justice's computer crime and intellectual property section, wrote online when the hacking allegations surfaced in March. "My instinct is that the CIA probably has a better claim to controlling access than the committee" because it owned the machines and retained the right to have IT people access the computers.

The exemption for investigative and intelligence activities—also cryptic—might lean in favor of the CIA, too. It is unknown "what makes an activity 'lawfully authorized,' because no court has interpreted that section. But it's possible that it applies and negates CFAA liability," said Kerr, currently a George Washington University law professor.

Brennan has merely apologized for his employees' actions and referred the IG report to an accountability board for potential disciplinary measures.

So, if this isn't a criminal matter—what's the punishment for the admitted wrongdoing? Loss of credibility in the public court of opinion, other former federal officials say.

The incident compounds the criticism that U.S. intelligence agencies hold too much information, following disclosures by ex-federal contractor Edward Snowden about sweeping surveillance of citizens' Internet and call records.

"What is clear is that this is a real setback for the CIA and, indeed, the intelligence community writ large as it tries to rebuild credibility and trust with Congress and the American people in the post-Snowden era," said retired Maj. Gen. Charles J. Dunlap, former Air Force deputy judge advocate general and now a Duke University law professor. "What must be especially frustrating to intelligence professionals is that their community will take another serious political hit, and this time for an easily avoidable, self-inflicted wound on an issue that I think could have been resolved in an unquestionably proper way."

The intelligence community continues to deal with the challenge of trust versus law, Fitzgerald said. The Senate episode "has echoes of the Snowden revelations where, even when the NSA was following the letter of the law, the actions were deeply unpopular, and out of step with the public's expectations or, in this case, the Senate's expectations," he said.

Justice Looks the Other Way

So far, the Justice Department reportedly has declined to proceed with a criminal investigation.

About a decade ago, after another government employee inappropriately searched congressional computers, Justice let him off the hook.

During President George W. Bush's first term, Senate Republican aide Manuel Miranda accessed documents belonging to the Committee on the Judiciary Democrats by exploiting a server glitch. He then leaked the files to the conservative press. Miranda resigned after he was found out. A Justice probe was launched, but no criminal charges were filed.

A redacted version of the intelligence panel's final torture report remains under wraps.

The CIA sanitized the report and Feinstein said Tuesday the omissions mask key evidence supporting the committee's conclusions.

"I am sending a letter today to the president laying out a series of changes to the redactions that we believe are necessary prior to public release," she said in a statement. "The bottom line is that the United States must never again make the mistakes documented in this report. I believe the best way to accomplish that is to make public our thorough documentary history of the CIA's program."

Critical Thinking

1. Is the argument that "there was no deliberate effort to inappropriately penetrate the system" a valid defense for the CIA? Why or why not?
2. Should matters pertaining to Homeland Security be treated as "above the law" if the CIA believes the situation necessitates them to be so? Explain.

Create Central

www.mhhe.com/createcentral

Internet References

New York Times: "Inquiry by C.I.A. Affirms It Spied on Senate Panel"

http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html?_r=0

TheJournal.ie: "CIA chief apologises to US Senate intelligence committee for agents hacking its computers"

http://www.thejournal.ie/cia-hacks-us-senate-computers-1599554-Jul2014/

Aliya Sternstein reports on cybersecurity and homeland security systems. She's covered technology for more than a decade at such publications as National Journal's Technology Daily, Federal Computer Week and Forbes.

Aliya Sternstein, "The CIA Can't Hack Senate Computers Because They Own Them, Experts Say," *defenseone.com*, August 7, 2014. Copyright © 2014 by National Journal Group. All rights reserved. Used with permission from Wright's Media.

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

How Technology is Transforming the Future of National Security

PATRICK TUCKER

Learning Outcomes

After reading this article, you will be able to:

- Discuss America's dwindling commitment to developing armed drone technology.
- Describe the Pentagon's interest in climate change.
- Identify the differences between quantum cryptography and pulse position modulation.

Transformative Technology and the Future of National Security

Maintaining technological superiority is a constant challenge for the military, one that U.S. Navy Rear Admiral Mathew Klunder, head of the Office of Naval Research, thinks about in personal terms. "I never want to see U.S. sailors or Marines in a fair fight." Keeping the fight unfair is more complicated than it has ever been. Despite some $63.5 billion of research and development funding allocated to the Defense Department in fiscal year 2015, the proliferation of cheap computers, cheap Internet and cheap drones is changing geopolitical realities faster than Washington can keep up.

This e-book on emerging technologies and their influence on national security seeks to provide a snapshot of the challenges and opportunities of the next several decades. We'll explore the military's ongoing efforts to use big data strategically in an environment where the NSA's data collection activities have provoked backlash from all corners. We'll examine the proliferation of unmanned aerial vehicles and its implications for the future of war and peace. We'll also look at the military's efforts to harness breakthrough technologies from atomic GPS to synthetic fuel and more. These articles are presented as conversation starters. The discussion of the technologies of tomorrow will be fast-moving in the months ahead, much like the pace of technological advancement itself. Whether or not the fight is fair, it's about to get a lot more interesting.

Every Nation Will Have Armed Drones by 2024

The proliferation of weaponized drone technology is inevitable, and there's nothing the U.S. can do to stop it.

Virtually every country on Earth will be able to build or acquire drones capable of firing missiles within the next 10 years. Armed aerial drones will be used for targeted killings, terrorism and the government suppression of civil unrest. What's worse, say experts, it's too late for the United States to do anything about it.

After the past decade's explosive growth, it may seem that the U.S. is the only country with missile-carrying drones. In fact, the U.S. is losing interest in further developing armed drone technology. The military plans to spend $2.4 billion on unmanned aerial vehicles, or UAVs, in 2015. That's down considerably from the $5.7 billion that the military requested in the 2013 budget. Other countries, conversely, have shown growing interest in making unmanned robot technology as deadly as possible. Only a handful of countries have armed flying drones today, including the U.S., United Kingdom, Israel, China and (possibly) Iran, Pakistan and Russia. Other countries want them, including South Africa and India. So far, 23 countries have developed or are developing armed drones, according to a recent report from the RAND organization. It's only a matter of time before the lethal technology spreads, several experts say.

"Once countries like China start exporting these, they're going to be everywhere really quickly. Within the next 10 years, every country will have these," Noel Sharkey, a robotics and artificial intelligence professor from the University of Sheffield, told *Defense One.* "There's nothing illegal about these unless you use them to attack other countries. Anything you can [legally] do with a fighter jet, you can do with a drone."

Sam Brannen, who analyzes drones as a senior fellow at the Center for Strategic and International Studies' International Security Program, agreed with the timeline with some caveats. Within five years, he said, every country could have access to the equivalent of an armed UAV, like General Atomics' Predator, which fires Hellfire missiles. He suggested five to 10 years as a more appropriate date for the global spread of heavier, longer range "hunter-killer" aircraft, like the MQ-9 Reaper. "It's fair to say that the U.S. is leading now in the state of the art on the high end [UAVs]" such as the RQ-170.

"Any country that has weaponized any aircraft will be able to weaponize a UAV," said Mary Cummings, Duke University professor and former Navy fighter pilot, in a note of cautious agreement. "While I agree that within 10 years weaponized drones could be part of the inventory of most countries, I think it is premature to say that they will. . . . Such endeavors are expensive [and] require larger UAVs with the payload and range capable of carrying the additional weight, which means they require substantial sophistication in terms of the ground control station."

Not every country needs to develop an armed UAV program to acquire weaponized drones within a decade. China recently announced that it would be exporting to Saudi Arabia its Wing Loong, a Predator knock-off, a development that heralds the further roboticization of conflict in the Middle East, according to Peter Singer, Brookings fellow and author of *Wired For War: The Robotics Revolution and Conflict in the 21st Century.* "You could soon have U.S. and Chinese made drones striking in the same region," he noted.

Singer cautions that while the U.S. may be trying to wean itself off of armed UAV technology, many more countries are quickly becoming hooked. "What was once viewed as science fiction, and abnormal, is now normal . . . Nations in NATO that said they would never buy drones, and then said they would never use armed drones, are now saying, 'Actually, we're going to buy them.' We've seen the U.K., France, and Italy go down that pathway. The other NATO states are right behind," Singer told *Defense One.*

Experts suggest its time the U.S. embrace the inevitable and put weaponized drone technology into the hands of additional allies

Virtually any country, organization, or individual could employ low-tech tactics to "weaponize" drones right now. "Not everything is going to be Predator class," said Singer. "You've got a fuzzy line between cruise missiles and drones movin forward. There will be high-end expensive ones and low-en cheaper ones." The recent use of drone surveillance and eve the reported deployment of booby-trapped drones by Hezbollah, Singer said, are examples of do-it-yourself killer UAV that will permeate the skies in the decade ahead—though mor likely in the skies local to their host nation and not over American cities. "Not every nation is going to be able to carry ou global strikes," he said.

Weaponized Drones Are Inevitable: Embrace It

So, what option does that leave U.S. policy makers wantin to govern the spread of this technology? Virtually none, sa experts. "You're too late," said Sharkey, matter-of-factly.

Other experts suggest that its time the U.S. embrace th inevitable and put weaponized drone technology into the hand of additional allies. The U.S. has been relatively constraine in its willingness to sell armed drones, exporting weaponize UAV technology only to the United Kingdom, according to recent white paper, by Brannen for CSIS. In July 2013, Congress approved the sale of up to 16 MQ-9 Reaper UAVs t France, but these would be unarmed.

"If France had possessed and used armed UAVs . . . whe it intervened in Mali to fight the jihadist insurgency Ansa Dine—or if the United States had operated them in support o otherwise passed on its capabilities—France would have bee helped considerably. Ansar Dine has no air defenses to counte such a UAV threat," note the authors of the RAND report.

In his paper, Brennan makes the same point more forcefull "In the midst of this growing global interest, the United State has chosen to indefinitely put on hold sales of its most capabl [unmanned aerial system] to many of its allies and partners which has led these countries to seek other suppliers or to begi efforts to indigenously produce the systems," he writes. "Continued indecision by the United States regarding export of thi technology will not prevent the spread of these systems."

The Missile Technology Control Regime, or MTCR, is probably the most important piece of international policy that limit the exchange of drones and is a big reason why more countries don't have weaponized drone technology. But China neve signed onto it. The best way to insure that U.S. armed drone and those of our allies can operate together is to reconsider th way MTCR should apply to drones, Brannen writes.

"U.S. export is unlikely to undermine the MTCR, whic faces a larger set of challenges in preventing the proliferation of ballistic and cruise missiles, as well as addressin more problematic [unmanned]-cruise missile hybrids such a so-called loitering munitions (e.g., the Israeli-made Harop)," he writes.

Weaponized, Yes. Weaponized and autonomous? Maybe.

The biggest technology challenge in drone development o promises the biggest reward in terms of cost savings d functionality: full autonomy. The military is interested drones that can do more taking off, landing and shoot- on their own. UAVs have limited ability to guide them- ves and the development of fully autonomous drones is rs away. But some recent breakthroughs are beginning to r fruit. The experimental X-47B, a sizable drone that can off of aircraft carriers, "demonstrated that some discrete ks that are considered extremely difficult when performed humans can be mastered by machines with relative ease," nnen notes.

Less impressed, Sharkey said the U.S. still has time to nink its drone future. "Don't go to the next step. Don't make m fully autonomous. That will proliferate just as quickly l then you are really going to be sunk."

Others, including Singer, disagreed. "As you talk about this ving forward, the drones that are sold and used are remotely oted to be more and more autonomous. As the technology omes more advanced it becomes easier for people to use. To a Predator, you used to need to be a pilot," he said.

'The field of autonomy is going to continue to advance ardless of what happens in the military side."

DARPA Projects That Could hange the World

RPA director Arati Prabhakar gives a preview of four of military's mad science projects that could change they way live.

Forty years ago, a group of researchers with military money out to test the wacky idea of making computers talk to one ther in a new way, using digital information packets that ld be traded among multiple machines rather than tele- nic, point-to-point circuit relays. The project, called ARPA- T, went on to fundamentally change life on Earth under its e common name, the Internet.

Today, the agency that bankrolled the Internet is called the ense Advanced Research Projects Agency, or DARPA, ch boasts a rising budget of nearly $3 billion split across programs. They all have national security implications but, the Internet, much of what DARPA funds can be commer- ized, spread and potentially change civilian life in big ways its originators didn't conceive.

What's DARPA working on lately that could be Internet ? Last week at the Atlantic Council, DARPA director Arati bhakar declined to name names. Like a good mutual fund ager, she said that her job was to "manage risk through rsity" in her portfolio. But the technologies that she high- ted in her recent testimony (PDF) to the Senate Appropria- s Committee look like a list of insider favorites. Many have received much less public attention than DARPA's flashier robot initiatives.

Here are four of DARPA's potential next big things:

1. Atomic GPS

The Global Positioning System, or GPS, which DARPA had an important but limited role in developing, is a great tool but maintaining it as a satellite system is increasingly costly. A modern GPS satellite can run into the range of $223 million, which is one reason why the Air Force recently scaled back its procurement.

DARPA doesn't have an explicit program to replace GPS, but the DARPA-funded chip-scale combinatorial atomic navigation, or C-SCAN, and Quantum Assisted Sensing, or QuASAR, initiatives explore a field of research with big relevance here: the use of atomic physics for much better sensing. If you can measure or understand how the Earth's magnetic field acceleration and position is effecting individual atoms (reduced in temperature), you can navigate without a satellite. In fact, you can achieve geo-location awareness that could be 1,000 times more accurate than any system currently in existence, say researchers.

The British military is investing millions of pounds in a similar technology. Researchers associated with the project forecast that they will have a prototype ready within five years.

The upshot for quantum navigation for any military is obvious. It arms them with better and more reliable situational awareness for soldiers and equipment and better flying for missiles. Perhaps, more importantly, a drone with a quantum compass wouldn't require satellite navigation, which would make it much easier to fly and less hackable.

The big benefit for everybody else? Future devices that understand where they are in relation to one another and their physical world won't need to rely on an expensive satellite infrastructure to work. That means having more capable and cheaper devices with geo-location capability, with the potential to improve everything from real-time, location-based searches to self-driving cars and those anticipated pizza delivery drones.

The most important civilian use for quantum GPS could be privacy. Your phone won't have to get signals from space anymore to tell you where you are. It would know with atomic certainty. That could make your phone less hackable and, perhaps, allow you to keep more information out of the hands of your carrier and the NSA.

2. Terehertz Frequency Electronics and Meta-Materials

The area of the electromagnetic spectrum between microwave, which we use for cell phones, and infrared, is the Terehertz range. Today, it's a ghost town, but if scientists can figure out how to harness it, we could open up a vast frontier of devices that don't compete against others for spectrum access. That would be a strategic advantage in a time when more military devices use the same electromagnetic spectrum space.

Research into THz electronics has applications in the construction of so-called metamaterials, which would lend themselves to use in cloaking for jets and equipment and even, perhaps, invisibility.

On the civilian side, because THz radiation, unlike X-ray radiation, is non-invasive, metamaterial smart clothes made with small THz sensors would allow for far faster and more precise detection of chemical changes in the body, which could indicate changes in health states. There's the future doctor in your pocket.

3. A Virus Shield for the Internet of Things

CISCO systems has forecast 50 billion interconnected devices will inhabit the world by the year 2020, or everything from appliances to streets, pipes and utilities through supervisory command and control systems. All of that physical and digital interconnection is now known as the Internet of Things.

The High Assurance Cyber Military Systems program, or HACMS, which DARPA announced in 2012, is trying to patch the security vulnerabilities that could pervade the Internet of Things. The agency wants to make sure that military vehicles, medical equipment and, yes, even drones can't be hacked into from the outside. In the future, some of the software tools that emerge from the HACMS program could be what keeps the civilian Internet of Things operating safely. This breakthrough won't be as conspicuous as the Internet itself. But you will know its influence by what does not happen because of it—namely, a deadly industrial accident resulting from a catastrophic cyber-security breach. (See: Stuxnet.)

This breakthrough won't be as conspicuous as the internet itself. But you will know its influence by what does not happen because of it.

Without better security, many experts believe the Internet of things will never reach its full potential. In a recent survey by the Pew Internet and American Life Project about the future of physical and digital interconnection, Internet pioneer Vint Cerf, who was instrumental in the success of ARPANET, said that in order for the Internet of things to really revolutionize the way we live it must be secure.

"Barriers to the Internet of Things include failure to achieve sufficient standardization and security," he said. HACMS could provide the seeds for future security protocols, allowing Internet of things to get off the ground.

4. Rapid Threat Assessment

The Rapid Threat Assessment, or RTA, program wants to sp
up by orders of magnitude how quickly researchers can
ure out how diseases or agents work to kill humans. Inst
of months or years, DARPA wants to enable researcher
"within 30 days of exposure to a human cell, map the comp
molecular mechanism through which a threat agent alters
lular processes," Prabhakar said in her testimony. "This wo
give researchers the framework with which to develop med
countermeasures and mitigate threats."

How is that useful right now? In the short term, thi
another research area notable primarily for what doesn't h
pen after it hits, namely pandemics. It took years and a lo
money to figure out that H5N1 bird flu became much m
contagious with the presence of an amino acid in a spec
position. That's what enabled it to live in mammalian lu
and, thus, potentially be spread by humans via coughing
sneezing. Knowing this secret earlier would have prevente
great deal of death.

In the decades ahead, the biggest contribution of the progr
may be fundamental changes in future drug discovery. "If s
cessful, RTA could shift the cost-benefit trade space of us
chemical or biological weapons against U.S. forces and co
also apply to drug development to combat emerging diseas
Prabhakar said.

Before any of these four reach Internet-level succ
DARPA faces a big challenge despite its continued popular
in that they remain a government agency at a time when cha
moves faster than the U.S. government understands.

"We move at a pace measured in decades in an envir
ment that changes every year," Prabhaka said, at the Atla
Council. In terms of the emerging technology she's most c
cerned about, it's the unknown unknowns, the U.S. militar
"ability to handle this vast changing landscape."

The agency that helped to bring about the Internet, Siri, a
GPS will always enjoy a certain cachet, warranted or not. I
the world moves faster than even DARPA can keep up. Perha
the most important thing that DARPA can create in the ye
ahead is manageable expectations.

How Big Data Could Track the Next Snowden

The U.S. wants intelligence workers put into a big data clo
they can monitor, and it just might work.

National Intelligence Director James Clapper, at a Febru
11 Senate Armed Services Committee hearing, asserted (aga

ke Edward Snowden, constituted a top threat to our nation's ational security. The lawmakers agreed and pressed Clapper to xplain how he was changing the practices within his office and cross the intelligence community to prevent another Snowden-cale data breach. One key step that Clapper outlined: our ation's top intelligence folks will become subject to much ore surveillance in the future.

Clapper said he wanted to put more intelligence community ommunication into a single, massive (enterprise-sized) cloud nvironment in order to, as he described it, "take advantage of loud computing and the necessary security enhancements" erein. There are plenty of good reasons for any department ead to want that, but chief among them for Clapper is that oving to the cloud will allow monitors to better "tag the data, nd] tag the people, so that you can monitor where the data is nd who has access to it on a real-time basis."

Anticipating insider threat behavior is a problem that governents have been wrestling with since the first act of state treason. ut the current round of research within the United States goes back efore Snowden to Army Pfc. Bradley (now Chelsea) Manning's 010 arrest for passing top-secret files to Wikileaks. Manning's isclosure prompted President Obama to issue Executive Order 3587, mandating the creation of an insider threat task force.

Mark Nehmer, associate deputy director of cybersecurity nd counterintelligence for the Defense Department, said that possible insider threat signal could include anything from a hange in marital status to a trip abroad to unusual online activ-y. One or two of these signals in isolation don't serve effec-vely as a red flag, but observed in the context of one another, atterns can emerge.

"Think of statistics and human behavior and think about orrelating past and future behavior, that's the future of insider reat, I believe," he said, at Nextgov's Cybersecurity Series in ashington on Tuesday.

Nehmer and several colleagues have offered DOD various ecommendations for curing the threat of an insider attack. hese include ensuring that more people with top secret clear-nce have at least one person sign off on work assignments volving sensitive information; stricter punishments for inor infractions involving data loss, glitches, and "spillage"; andating that all software fixes comply with a single new stan-rd; and the creation of a joint information environment (JIE) lowing all of the services to share information in one secure oud setting and far more effective monitoring of employee mmunication and activity.

"We have all these titanium silos of excellence and we rep-ate all these services and people. That's not getting us very r," Nehmer said, regarding the importance of the JIE. "We ed to build an architecture so that a whole department can e enterprise services." The Pentagon already has a JIE in place for e-mail said Nehmer. This will be extended across other military branches soon.

The question becomes, what are the Snowden-like signals to watch for in this new, more transparent environment?

Few people involved in insider threat programs in Washington are eager to talk about what makes a potential traitor conspicuous, but several interesting findings have been published out of Palo Alto, California.

Oliver Brdiczka, a researcher at PARC, and several of his colleagues have set up a number of experiments to observe potential insider threat behavior in closed online environments. In the first of these [PDF], Brdiczka looked at the massively multiplayer online game *World of Warcraft*. The game, which allows users to build characters, join large organizations called guilds, and go on missions and assignments, has been in the news a bit recently after the Snowden leaks revealed that the NSA had been listening in on chat room conversations between *World of Warcraft* players in the hopes of catching potential terrorists.

Brdiczka and his colleagues were after a more ambitious prize—a scientific understanding of how insider threats actually develop in realtime. Players hunting dragons and orcs wind up collaborating with team mates, applying for positions and earning rewards in somewhat the same way that work teams go about attacking big projects. The game thus served as a suitable proxy for a real world work environment. A player who quits her guild has the potential to damage it, perhaps even absconding with goods in much the same way that Edward Snowden defected with flashdrives of classified information. In Brdiczka's experiment, quitting served as a useful stand in for insider-threat behavior.

The researchers found volunteers, looked at each subject's social network presence, and made each fill out a personality survey. They then carefully observed how the players approached the game play, how they acquired items, fought monsters, interacted with one another and performed dozens of other tasks. Result: The researchers found that they could predict who was going to quit in six months with an accuracy rate of 89 percent.

Shortly after the test, Brdiczka and his colleagues expanded the research [PDF] to the real world. They looked to determine if e-mail patterns could predict quitting (attrition) and began by examining two data sets, a small company of 43 employees and a large company of 3,600, for a period of about 20 weeks. They measured everything from the frequency of e-mail to the time of day it was sent, to whether the e-mail had attachments or came as a forward. They even taught a computer program to categorize the tone in the messages as being positive or negative. In the end, the results of the experiment were a bit less conclusive than the *World of Warcraft* study. They were able to predict quitting with about 60 percent accuracy.

But they did find some important clues that can predict potential insider threat behavior, and they were counterintuitive. The team had expected that the strongest signal of a quitting event would be e-mails with a highly negative tone, full of spit and spite. In fact, the best attrition symptom was fewer e-mails fewer messages after hours, fewer attachments, fewer words all together.

The Snowden in your office is the guy going dark.

Brdiczka's work is currently being funded by a grant from the Defense Advanced Research Projects Agency, or DARPA. The goal of the Anomaly Detection at Multiple Scales, or ADAMS, program is to "create, adapt, and apply technology to the problem of anomaly characterization and detection in massive data sets. . . . The focus is on malevolent insiders that started out as 'good guys.' The specific goal of ADAMS is to detect anomalous behaviors before or shortly after they turn."

Of course, polls indicate public ambivalence as to whether Edward Snowden is a malevolent insider, a "good guy," or something else entirely. Also, varying bodies have differing definitions of what constitutes an insider in a military context. From a purely technological perspective, these aren't critical points to the functioning of an insider threat computer model. Brdiczka told me that, with some small modification to account for different feature sets, the model could scale up to apply to virtually any domain where online social interaction can be observed and measured. That includes the JIE that the Pentagon wants to build across all service branches, or, for that matter, all of Facebook.

Congratulations. You're an insider now.

The Military is Planning for Climate Change

While the rest of the world continues to debate climate change, the Pentagon has long been preparing for a more unstable environment.

The White House released its National Climate Assessment this May, a 1,100 page document by more than 300 experts examining the effects of man-made climate change on various aspects of American life. While 97 percent of climate scientists agree that climate change is occurring and that human factors are largely the cause, public debate persists around climate change, humanity's role in it, and whether or not its effects will be as severe as the Obama administration and the scientific community are projecting.

But there's little debate over climate change at the Pentagon, where the realities of temperature increases are now a part of everyday planning.

"We have to be concerned about all of the global impacts [of climate change], including here at home, where the Defense Department does have a mission in supporting civil authorities in the event of natural disasters. We have to be concerned about all of it," Sharon Burke, Assistant Secretary of Defense for Operational Energy Plans and Programs told *Defense One*.

"We have to be pragmatic about it," Burke said. "The question is, how is this changing facts on the ground? If we're seeing salt water intrusion at an aquifer at a base in North Carolina, we have to deal with it."

The report's broadest points mirror those of the 2013 Intergovernmental Panel on Climate Change: There will be a rise in global temperature that varies significantly depending on how much more CO2 is released into the atmosphere in the coming decades. Projections vary from a few degrees' rise to more than 10 degrees by the year 2100. The hottest days of the year would be as much as 15 degrees hotter on average. Sea levels could rise by as much as four feet.

Not everyone agrees with the dire assessment. Paul Knappenberger and Patrick Michael of the CATO Institute were quick to dismiss the report as "biased toward pessimism." "The report overly focuses on the supposed negative impacts from climate change while largely dismissing or ignoring the positives from climate change," they said.

"I'm not seeing intransigence [on the issue] in the Pentagon," retired Army Brig. Gen. John Adams told *Defense One*. Adams is an advisor to the Center for Climate Security, which looks at the intersection of climate change and national security. 'The Pentagon is seeing this as a problem. Instability is accelerating. Climate change is an accelerator of instability. The Pentagon understands that. They're looking at what sorts of force structures and equipment they're going to need to have available to deal with increasing instability that will be most effected by climate change."

Adams, who lives in Pensacola, Fla., spoke specifically about how climate change is influencing military decision-making near him. "We have major installations in this area. We predict the sea level will rise here. That means that Navy ship berths will have to change, because they're not floating docks, they're built into the land. And when the sea level rises above the point where it's safe to berth a Navy ship, then you have to change the berthing structure . . . so climate change will have an effect on our basing structures."

Climate change will also alter the way the military acquires equipment, Adams said. "If we're going to find ourselves operating in littoral areas that are affected by climate change, where the instability will be most accelerated by climate change, we have to have the force structure to be able to operate."

The White House report makes note of the changing arctic as a future destination for increased U.S. naval activity. "With sea ice receding in the Arctic as a result of rising temperatures, global shipping patterns are already changing and will continue to considerably in the decades to come."

It's also a concern that Defense Secretary Chuck Hagel reiterated in a major speech in Chicago in May. "The melting of ntic ice caps presents possibilities for the opening of new anes and the exploration for natural resources, energy, and merce. The Defense Department is bolstering its engage- in the Arctic and looking at what capabilities we need to ate there in the future," he said at the Chicago Council on al Affairs.

dams says "there will be new competitors for that route. United States has a big role to play in any of the sea lanes."

limate change is already influencing the military mission, e said, as the U.S. builds up its military-to-military ionships around the world. "We had 14,000 people who oyed to support [relief] efforts for Hurricane Sandy. We had a lot of people who deployed to support relief efforts the typhoon in the Philippines. We're already seeing ased demands on our time," she said.

hile the military faces the effects of climate change head t also contributes to the problem. In 2013, the Defense rtment burned more than 12 million gallons of oil a day. the department has also offered some potential solutions ilitary dependence on fossil fuels. The Office of Naval arch recently announced the successful creation of a syn- c fuel from seawater. But much of the innovation taking e to green the military is far more subtle. DOD plans to t $1.7 billion in fiscal year 2015 on initiatives to improve gy efficiency and energy performance, Burke said.

limate and weather has been part of the military conver- n since the dawn of armies, but the current conversation een the Obama administration and the military is rooted in 010 Quadrennial Defense Review, which observed: "DOD need to adjust to the impacts of climate change on our facil- and military capabilities. . . . While climate change alone not cause conflict, it may act as an accelerant of instabil- r conflict, placing a burden to respond on civilian insti- ns and militaries around the world. In addition, extreme her events may lead to increased demands for defense sup- to civil authorities for humanitarian assistance or disaster nse both within the United States and overseas."

e next National Climate Assessment is due within four s and will look squarely at the national security implica- of climate change. "Right now everyone is looking at h, environment, and economy and how those things fit her and those are really important. But we also feel it's d time to look specifically at security," Burke said. "I do there's a dialogue between the scientists, engineers, and ymakers to have actionable information. That's a conver- n that needs to deepen."

e Most Secure E-mail in the Universe

's how you will one day be able to send invisible messages ur future quantum cell-phone.

Say you wanted to send an e-mail more secure than any message that had ever been transmitted in human history, a message with *absolutely* no chance of being intercepted. How would you do it?

You may have encrypted your message according to the highest standards, but encryption doesn't guarantee secrecy. The fact that you sent it is still detectable. An intercepting party in possession of just a few clues such as your identity, the receiver's identify, the time of the message, surrounding incidents and the like can infer a great deal about the content of the message in the same way that the NSA can use your metadata to make inferences about your personality. You need to conceal not just what's in the message but its very existence.

The answer? Make your message literally impossible to detect. A team of researchers from the University of Massachusetts at Amherst and Raytheon BBN Technologies led by Boulat A. Bash have created a method for doing just that, cloaking electronic communications so that the communication can't be seen. They explain it in a paper titled Covert Optical Communication.

The question of exactly how secure any communication can be is of no small relevance either to national security watchers worried about losing secrets or to a public increasingly concerned about governmental invasion of digital privacy. The breakthrough shows that it is possible to send a message that can't be intercepted, no matter how determined the National Security Agency is to intercept it.

The practice of embedding secret messages in computer files is called digital steganography. Steganography has been around since the days of ancient Greece. The term simply refers to the deliberate hiding of a message within a message. Dissidents in Laos, the United Arab Emirates, Saudi Arabia, and especially China use *digital* steganography to send secret messages. But these methods are far from fully secure.

Today, we send a lot of messages over fiber-optic cable, essentially using light as a communications medium. It's instant and cheap but someone monitoring the photons passing through those cables can detect when one party is sending a message to another (it is just *light,* after all.) Photon detectors are extremely accurate, able to detect single photons passing between two points, but they aren't perfect and sometimes they read false positives. Bash's technique makes use of that flaw using pulse position modulation—and it's not much more complicated than Morse code.

Take a unit of time, like a second, and chop it up into smaller parts that vary in size, one-fourth, one-eighth, and so on. Then assign each band a corresponding symbol. There's your code. You can transfer a photon-based message over a fiber-optic capable that corresponds to the code and—so long as the message sender and the receiver of the message both have the key to the code—then each can read the message.

Pulse position modulation is not new. The formula that Bash and his colleagues created takes this process to the next step rendering it far more useful. It solves for how many bits of message a sender can pack into a certain interval of time in order for the message to always appear like background noise to any detector currently in existence.

In addition to light-based communication, the formula would render undetectable cell phone-based text messages. Cell phones use microwaves to send and receive data, which is a very noisy area of the electromagnetic spectrum. More noise is good in Bash's communication-concealing scheme in the same way that it's easier to hide in dense jungle foliage than it is in open desert.

Unfortunately, you and the person you are sharing the message with must agree in advance on the code and exchange it, which presents something of an obstacle.

While there is no way to share a secret code in an invisible e-mail there is a way to share it in an encrypted e-mail that would destroy itself if viewed by an outsider. Using quantum encryption, you could send a message between two parties containing the deciphering key and that message, while detectable, would also be unhackable.

University of Oxford quantum physicist Artur Ekert calls quantum encryption the ultimate physical limits of privacy. Other key distribution schemes such as the Diffie Hellman scheme, rely on the difficulty of mathematical problems to work, whereas quantum encryption does not. According to Heisenberg's uncertainty principle, objects viewed on the atomically small quantum scale change their behavior when viewed. Quantum encryption offers the possibility of a message so secure that any attempt to read it without authorization will destroy it, not because of some programmer's whim but because of the way subatomic particles operate.

"For quantum cryptography we need 'only' to transit quantum particles over a certain distance, and this is relatively easy. Quantum cryptography has been demonstrated in practice and there are even companies that can sell it to you," Ekert told *Defense One*.

Quantum cryptography and Bash's pulse position modulation technique are two very different animals. Cryptography makes messages difficult to decipher and pulse position modulation cloaks them so that they can't be detected. But Bash's method could go hand-in-hand with something like quantum key distribution, which a message sender would use in advance to share the key code. That, in turn, would be used in the future for covert communication.

Here's what the most secure electronic message exchange in the history of humanity would look like: You would first exchange the code key in a quantum encrypted message, and then, when the receiver and the sender both had the code, they could exchange an invisible—thus perfectly secure—message. A third party might be able to detect that two parties had exchanged a single message that had been quantum encrypted, containing the key code, but that third party wouldn't be able to see any of the exchanges that passed after that or open the key code message.

The breakthrough shows that it is possible to send a message that can't be intercepted, no matter how determined the national security agency is to intercept it.

Right now, quantum encryption is not the sort of service you can use on your iPhone or some common device. It requires dedicated devices and a connection between two points. But that will change, according to Ekert. "We will probably demonstrate device independent quantum crypto soon in the labs, but it will take some time before we turn them into a commercial proposition," he said.

How soon? Perhaps sooner than many think. Back in August, members of a team from the University of Bristol published a paper outlining ideas for how to do it.

Secure? Yes. Practical for all communication? No. Bash's method is not one you would use for everything. The laws of physics that make photon cloaking possible impose a stingy limit on the size of the message that is transferable over that medium, limited to tens to hundreds of bits of per second according their paper. That's enough space to send yes or no signals or small values, but sending an entire Word document at that rate would take a very long time.

The NSA is spending nearly $80 million on a program called Penetrating Hard Targets to build a quantum computer to de-encrypt the most expertly encoded communications, according to *The Washington Post*. The government has been funding quantum computer research for more than a decade to develop techniques for super hacking. So far, the record suggests that they have little to show for their efforts.

"Purely on numbers, the agency would appear to be lagging behind major labs such as the Institute for Experimental Physics at the University of Innsbruck in Austria," noted Jon Cartwright in a recent piece for *Physics World*.

Despite the agency's reputation for digital omnipresence, their real capabilities are far from godlike.

"The recent Snowden revelations confirm something we've long suspected: NSA does not really have a supercomputer that can break all of our standard cryptography. What they've resorted to is colluding with equipment manufacturers to include 'back doors' in encryption products and software," Johns Hopkins University cryptology expert Matthew Green told *Defense One*, referring to the recent revelations that the NSA had given security industry provider RSA multiple encryption tools. "All of this discussion about quantum crypto is moot if someone puts a back door into the hardware responsible for performing he encryption."

For the majority of the public, the best way to secure your personal e-mail is to use some commonly available tools, Green said.

"Our current practical encryption schemes are all extremely ecure, and there's no reason to believe that your communications aren't confidential—provided you're using encryption and it's properly implemented," he said. "In theory, these chemes can be broken, but the computational effort to do it is ar beyond what humans will ever muster."

Critical Thinking

1. Use an example to illustrate why the "upshot for quantum navigation for any military is obvious."
2. Is it a practical suggestion that "more people with top secret clearance" have at least one person sign off on work assignments involving sensitive information? Why or why not?
3. Which of the public's ambivalent assessments of Edward Snowden is most appropriate: he is a malevolent insider, a "good guy," or something else entirely? Explain.

Create Central

www.mhhe.com/createcentral

Internet References

engadget: "Google tests the performance limits of D-Wave's quantum computers"

http://www.engadget.com/2014/01/20/googie-tests-the-performace-limits-of-d-wave-quantum-computers/

International Committee of the Red Cross: "The use of armed drones must comply with laws"

https://www.icrc.org/eng/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm

New York Times: "Pentagon Signals Security Risks of Climate Change"

http://www.nytimes.com/2014/10/14/us/pentagon-says-global-warming-presents-immediate-security-threat.html?_r=0

Popular Science: "DARPA To Scientists: Find A Better Way To Study Chemical Weapons"

http://www.popsci.com/technology/article/2013-05/darpa-scientists-find-better-way-study-chemical-weapons

RT: "Pentagon increasing surveillance to prevent another Snowden-style leak"

http://rt.com/usa/188824-pentagon-intelligence-monitoring-leak/

Patrick Tucker is technology editor for *Defense One*. He's also the author of *The Naked Future: What Happens in a World That Anticipates Your Every Move?* (Current, 2014). Previously, Tucker was deputy editor for *The Futurist*, where he served for nine years. Tucker's writing on emerging technology also has appeared in *Slate, The Sun, MIT Technology Review, Wilson Quarterly, The American Legion Magazine, BBC News Magazine* and *Utne Reader* among other publications.

rick Tucker, "How Technology is Transforming the Future of National Security," *defenseone.com*, July 2014. Copyright © 2014 by National Journal Group. All rights reserved.
ed with permission from Wright's Media.

Article

Prepared by: Caroline Shaffer Westerhof, *California National University for Advanced Studies*

Deception Is Futile When Big Brother's Lie Detector Turns Its Eyes on You

ADAM HIGGINBOTHAM

Learning Outcomes

After reading this article, you will be able to:

- Understand the role of technology in lie detection; articulate several approaches to using technology to support lie detection and the relative success of each.
- Understand the role of politics in determining which technologies are funded for research and development.
- Articulate both advantages and disadvantages of having avatars conduct initial border screenings.

Alan Bersin, commissioner of Customs and Border Protection, arrives at the gloomy US border post in Nogales, Arizona, early one winter morning wearing an expression of mildly pained concentration.

He got up before dawn and now looks as if he'd rather be anywhere else. In the immigration lanes downstairs, a procession of pickups and SUVs nudge dejectedly in from Mexico, taillights blinking through a relentless drizzle. Bersin arrived late, and he seems in no mood to assess the state of the art in automated psychophysiological evaluation technology. Yet there it is, pushed up against the wall of a cramped back office at the DeConcini Port of Entry: a gray metal box about the size and shape of an ATM, with two softly glowing video monitors, one on top of the other.

Bersin, a self-assured bureaucrat and a Rhodes Scholar who studied at Oxford with Bill Clinton, approaches the device. The lower monitor displays an icon of an oversize red button; the upper screen shows the head and shoulders of a smoothly rendered, computer-generated young man blinking and occasionally suffering a slight electronic shudder. He appears to be in his twenties and has an improbably luxuriant head of blue-black hair combed back in a sumptuous pompadour. This is the Embodied Avatar, the personification of the latest software developed to help secure the nation's frontiers by delivering what its creator calls "a noninvasive credibility assessment"—sifting dishonest travelers from honest ones. Which is to say, this late-model Max Headroom is a lie detector.

Bersin taps the red button to start the test, and in an agreeable Midwestern voice, the avatar asks Bersin a series of questions.

"Are you a citizen of the United States of America?"

"Yes," Bersin says.

"Have you visited any foreign countries in the past five years?"

"Yes."

"Do you live at the address you listed on your application?"

"Yes."

When the interview is over, Bersin turns to the other people in the room—his entourage, a delegation from the Canadian border agency, and the engineers who are anxiously overseeing this most critical test yet of their invention.

One technician explains to Bersin how the kiosk has instantly analyzed his responses, displayed on a rubber-jacketed iPad and broken down into categories of risk: green, yellow, and red. Bersin's mask of barely suppressed boredom does not crack.

But then the technician points out that one of his answers is flagged in red: The machine is suspicious about his address. Bersin acknowledges that, yes, what he usually describes as his home is not actually where he lives, and that he was thinking about something else when he was answering—it's just that he has a work residence in Washington, DC, but of course his family home remains back in San Diego and—

Bersin's counterpart from Canada, a former intelligence officer, interrupts, cracking an interrogator's indulgent smile: "Do you have a lawyer?"

Afterward, Jay Nunamaker, the sardonic computer engi-
r overseeing the Embodied Avatar project, allows himself a
chuckle. "I don't think it could have gone better," he says.
thin a few hours, the young man with the improbable hair
nterviewing members of the public. The first field tests of
US government's state-of-the-art computer-controlled lie-
ection device have begun.

Since September 11, 2001, federal agencies have spent
lions of dollars on research designed to detect deceptive
avior in travelers passing through US airports and border
ssings in the hope of catching terrorists. Security personnel
e been trained—and technology has been devised—to iden-
, as an air transport trade association representative once put
"bad people and not just bad objects." Yet for all this invest-
nt and the decades of research that preceded it, researchers
tinue to struggle with a profound scientific question: How
you tell if someone is lying?

That problem is so complex that no one, including the engi-
rs and psychologists developing machines to do it, can be
tain if any technology will work. "It fits with our notion of
ice, somehow, that liars can't really get away with it," says
ria Hartwig, a social psychologist at John Jay College of
minal Justice who cowrote a recent report on deceit detec-
at airports and border crossings. The problem is, as Hartwig
lains it, that all the science says people are really good at
g, and it's incredibly hard to tell when we're doing it.

In fact, most of us lie constantly—ranging from outright
s to minor fibs told to make life run more smoothly. "Some
he best research I've seen says we lie as much as 10 times
ry 24 hours," says Phil Houston, a soft-spoken former CIA
rrogator who is now CEO of QVerity, a company selling
detecting techniques in the business world. "There's some
earch on college students that says it may be double and
le that. We lie a ton." And yet, statistically, people can tell
ether someone is telling the truth only around 54 percent of
time, barely better than a coin toss.

he Interrogation Bot

three sensors tell the Embodied Avatar kiosk everything
eeds to know about whether someone is telling the truth.
infrared camera records eye movement and pupil dilation
p to 250 frames per second—the stress of lying tends to
se the pupils to dilate. A high-definition video camera cap-
s fidgets such as shrugging, nodding, and scratching, which
to increase during a deceptive statement. And a micro-
ne collects vocal data, because lies often come with minute
nges in pitch. Future versions of the machine might go even
her—a weight-sensing platform could measure leg and foot
ts or toe scrunches, and a 3-D camera could track the move-
ts of a person's entire body.—*Sara Breselor*

For thousands of years, attempts to detect deceit have relied on the notion that liars' bodies betray them. But even after a century of scientific research, this fundamental assumption has never been definitively proven. "We know very little about deception from either a psychological or physiological view at the basic level," says Charles Honts, a former Department of Defense polygrapher and now a Boise State University psychologist specializing in the study of deception. "If you look at the lie-detection literature, there's nothing that ties it together, because there's no basic theory there. It's all over the place."

Despite their fixation on the problem of deceit, government agencies aren't interested in funding anything so abstract as basic research. "They want to buy hardware," Honts says. But without an understanding of the mechanics of lying, it seems that any attempt to build a lie-detecting device is doomed to fail. "It's like trying to build an atomic bomb without knowing the theory of the atom," Honts says.

Take the polygraph. It functions today on the same principles as when it was conceived in 1921: providing a continuous recording of vital signs, including blood pressure, heart rate, and perspiration. But the validity of the polygraph approach has been questioned almost since its inception. It records the signs of arousal, and while these may be indications that a subject is lying—dissembling can be stressful—they might also be signs of anger, fear, even sexual excitement. "It's not deception, per se," says Judee Burgoon, Nunamaker's research partner at the University of Arizona. "But that little caveat gets lost in the shuffle."

The US Army founded a polygraph school in 1951, and the government later introduced the machine as an employee-screening tool. Indeed, according to some experts, the polygraph can detect deception more than 90 percent of the time—albeit under very strictly defined criteria. "If you've got a single issue, and the person knows whether or not they've shot John Doe," Honts says, "the polygraph is pretty good." Experienced polygraph examiners like Phil Houston, legendary within the CIA for his successful interrogations, are careful to point out that the device relies on the skill of the examiner to produce accurate results—the right kind of questions, the experience to know when to press harder and when the mere presence of the device can intimidate a suspect into telling the truth. Without that, a polygraph machine is no more of a lie-detector than a rubber truncheon or a pair of pliers.

As a result, although some state courts allow them, polygraph examinations have rarely been admitted as evidence in federal court; they've been dogged by high false-positive rates, and notorious spies, including CIA mole Aldrich Ames, have beaten the tests. In 2003 the National Academy of Sciences reported that the evidence of polygraph accuracy was "scanty and scientifically weak" and that, while the device might be used effectively in criminal investigations, as a screening tool it was practically useless. By then, other devices and techniques that had been touted as reliable lie detectors—voice stress analysis, pupillometry, brain scanning—had also either been dismissed as junk science or not fully tested.

But spooks and cops remain desperate for technology that could boost their rate of success even a couple of points above chance. That's why, in 2006, project managers from the Army's polygraph school—by then renamed the Defense Academy for Credibility Assessment—approached Nunamaker and Burgoon. The government wanted them to build a new machine, a device that could sniff out liars without touching them and that wouldn't need a trained human examiner: a polygraph for the 21st century.

A former college wrestler from Pittsburgh, Nunamaker is a leathery 75-year-old who trained as a mechanical engineer, and his methodical approach to problem-solving has carried him through four decades of developing software. He became interested in deception in the '90s, while building teleconferencing and collaboration software for corporate-scale behemoths including IBM and the US Army and Air Force. His clients suspected that many of their employees' contributions were often deliberately misleading, warped by self-interest and interdepartmental rivalry. Nunamaker discovered that he could pick out liars by looking for a statistical prevalence of evasive language and "hedging words," and he became fascinated with the ways deceitful employees betray themselves.

Burgoon, 64, a brisk and polished psychologist with cropped silver hair, had already done a decade of military-funded deception-detection work when she began collaborating with Nunamaker 12 years ago—both were at the University of Arizona working, it turned out, on similar projects. Burgoon specialized in examining deceit as part of interpersonal communication, a laborious, time-consuming, and—compared with the twitching needles and brain scanning at the other end of the field—unglamorous area of research. Nunamaker suggested they collaborate; her psychology background complemented his engineering expertise.

Instead of simply measuring signs of physiological arousal, Burgoon analyzed liars' body movement—expressions and gestures—and linguistic cues. Like Nunamaker, she had established that liars tend to hedge, equivocate, or fail to deny things directly. One recent study, using publicly available recordings of 911 calls from Florida and Ohio, found that using vague language about things like location and details of the crime often correlated with the caller being the perpetrator. Other research has shown that dishonest stories tend to be better structured than honest ones, although in the end the true story may seem more coherent. True narratives feature richer sensory detail, more direct speech, and more spontaneous corrections. "Deceivers are not going to say, 'Well, I can't remember that, I forgot that,'" Burgoon says. "They'll make something up."

For years, Burgoon collected linguistic data the hard way, transcribing interviews and marking them up by hand. Analyzing body movement was even more painstaking. Trained coders watched video of experimental subjects for hundreds of hours and logged each cue they saw—one blink, a slight smile—manually, using a pen and paper. One research project involved 300 videotaped interviews; the coding took three years. Analyzing the audio was even harder. Burgoon worked with specialists who attempted to hear the changes in vocal pitch in individual phonemes, the units of sound that make up words. Expanding to whole conversations proved almost impossible. "They were used to dealing with a phoneme, not with an entire utterance, much less an entire interview," Burgoon says.

When they first began working together in 2000, Nunamaker found it hard to believe that nobody had tried using machines to simplify this data collection. "It drove me crazy," he says. So Burgoon and Nunamaker started tracking body movement with software that superimposed computer-generated blobs over the video of interviewees; now computer vision tools can find a human being in an image and track more than 80 different landmarks on the face alone. Using transcripts of interviews with indicted Air Force personnel—whose lies were pretty well documented—they worked on artificial-intelligence tools to analyze language, counting hedging words and tracking pronoun use. (This evolved into a suite of software Burgoon dubbed the Agent99 Analyzer—she liked the idea of naming it after the female sidekick from *Get Smart*, famously more competent than her male boss.)

Eventually, Nunamaker and Burgoon came to believe that no single technology could solve the problems of lie detection. "There is no silver bullet answer—which is what everybody wants," Nunamaker says. "It's going to be this basket of cues and figuring out whether you've got the right cues in the basket." But they also knew that computers could detect the signs they'd identified. The researchers decided to combine as many sensors as possible in a single lie-detecting toolbox. By monitoring potentially hundreds of different psychophysiological, linguistic, and verbal cues, their hypothetical machine would spot tells in even the most polished liar. "A human can only control three or four at a time—so cues leak out no matter how hard you try," Nunamaker says.

One of the first government agencies interested in Nunamaker and Burgoon's work was the Department of Homeland Security. DHS paid for early data collection at the border station at Nogales, a project in which the researchers filmed travelers during screening interviews and then compared their linguistic and physical cues to the way customs officers rated them after screening. But the Science and Technology Directorate at DHS believed that even a working lie detector wouldn't be good enough to fight terrorism. They didn't just want to know when someone was lying—they wanted to look for signs that e person intended to do bad things, or "malintent." So before inamaker and Burgoon finished their fieldwork in Nogales, ey say, DHS asked them to abandon it and instead study the ationship between emotions, physical cues, and malintent—ecifically incorporating the microexpression theories of Paul man.

Ekman is a divisive figure. Now 78, his work on lie detecn has made him a rock star among behavioral psychologists, th a best-selling book, a profitable consulting business, and network TV drama—*Lie to Me*—inspired by his research. 1969 he theorized that facial muscles that expressed seven man emotions also created "microexpressions" that could eal concealment, despite the fact that these microexpresns last just 0.04 second. Ekman claims that with his training, possible to spot microexpressions and successfully detect ception 70 percent of the time, increasing this to almost 0 percent if other body movements are taken into account.

In 2006 Ekman and his team spent 30 days training TSA icers to read microexpressions as part of a program called OT—Screening Passengers by Observational Techniques. ese officers deployed to 161 airports across the US. Accord- to the TSA, from January 2006 through March 2012, SPOT icers referred more than 331,280 travelers for secondary eening, but the merest fraction were arrested—just 2,270. In time, at least 16 people involved in terrorism cases passed challenged through airport checkpoints manned by SPOT sonnel—some of them more than once. Nobody outside TSA knows what SPOT officers are looking for, since the ails remain classified. The agency admits to being uncertain it has yet detained a single terrorist. Charles Honts, who trained by Ekman, says that all his attempts to replicate man's experiments have failed, and in 2009 the researchers dying airports and border crossings found no evidence that roexpressions reliably betray concealed emotion or can be d to detect deceit. The next year the Government Accountity Office reported that the TSA's scheme had never been ntifically tested. (Ekman disputes these criticisms. Of the hijackers, for example, he says, "If the behavior that peoreported them showing did occur, it would certainly have picked up by SPOT.")

Nunamaker and Burgoon didn't want to abandon their dwork, and they didn't want to focus on microexpressions. ere's not a lot of science to back up Ekman's claims," Nunker says. "Applying them to deception detection is a reach." project manager pulled their funding—because, Nunaker says, he wouldn't switch the focus of his work. DHS ed ahead with Ekman's research. The new behavioral foreng program—Future Attribute Screening Technology—is ecret that even Burgoon has no idea what it does.

After falling out with DHS, Nunamaker and Burgoon sed on. They won new funding from the Pentagon and other agencies. Customs and Border Protection, for example, wanted to help overburdened customs officers screen immigration lines at borders, so the two decided to combine their lie-detecting toolbox with an idea other deception researchers were already playing with: a computer-generated interrogator.

An avatar interrogator has many advantages over its human counterparts. It's consistent, tireless, and susceptible to neither persuasion nor bribery. Douglas Derrick, a researcher at the University of Nebraska who studies human-computer interaction and has worked on the Embodied Avatar since 2007, even suspects that people fear the power they feel it embodies. "They view it as the personification of the system," Derrick says. "They believe they're talking to the computer." One early version was a menacing shaven-headed character nicknamed Scary Guy. On the other hand, Nunamaker says, Las Vegas casinos, which fund their own deception research to catch cheats, have had more success giving casino-goers screen-based directions and advice with avatars that resemble cartoons. Derrick even tried using a camera and morphing software so that an avatar would increasingly resemble the person in front of it, reflecting research that suggests you're more likely to trust someone who looks like you. The one thing they all had in common was skirting the edges of the uncanny valley, where characters look just human enough to be disturbing. "I think we're close with this one," Derrick says of the thick-haired young man used in Nogales. "It's realistic, but we're not in the valley."

The team dug into commercially available lie-detection technology, but most proved unusable. A thermal-imaging camera was enormous and required a cooling fan so noisy that it drowned out the other equipment. The laser Doppler vibrometer, which could monitor blood pressure from 10 feet away, could be circumvented by anyone wearing a turtleneck or even a beard. And the lie/truth analyzer, built into vocal dynamics software provided by the Israeli company Nemesysco, was hopeless under experimental conditions.

Despite those failings, Nunamaker and Burgoon thought that some of the gadgets had potential. Arizona grad student Aaron Elkins found that the Nemesysco software really was finding a correlation between vocal stress and deception, so he wrote his own algorithms to do the same thing—to measure cues like hesitation, changes in tempo and intonation, and spoken errors. It worked; Elkins' approach can identify deceitful speech 75 percent of the time in an experimental setting, and speech dynamics now provide key data points used by the technology being tested in Nogales.

Now, using just three sensors, they can collect as many as 50 different psychophysiological and vocal deception cues. A microphone gathers vocal information. An HD video camera captures body movement—for example, the sudden freezing of a liar attempting to control physical tells. And an infrared camera monitors pupil dilation and gaze pattern. Some of the team's most successful experiments have shown that eye flicker correlates to deception: Examining images of falsified documents, for example, subjects often cannot help looking repeatedly at the details they've doctored.

Separately, these streams of data can provide a good picture of when test subjects might be lying—in the lab, information from the eyes alone correctly flagged liars 60 percent of the time. But when the avatar kiosk combines the data from eye and voice analysis, its accuracy spikes. In an experiment in Poland last year using 37 EU border guards, some of whom were asked to present false documents, the kiosk identified every one of the liars. Taking into account two false positives, the machine scored 94 percent. Human agents asked to perform the same task failed to stop a single impostor.

Yet the success of such experiments has depended on the context of the interrogation. In October 2011, as Nunamaker's team began readying a version of the device for the field tests in Nogales, he admitted that he still wasn't certain how it would perform in the outside world: "We really don't know, until we test it at the border with real people who don't have a vested interest in the system working."

Two months later in Nogales, a uniformed customs officer introduces the avatar kiosk to the public for the first time. In line are a mother and daughter from Tucson, a well-dressed couple from over the border in Mexico, and a portly retiree in a baseball cap there to renew his trusted-traveler card. Each is here as part of a fast-track border crossing program and is first screened by a cheerful immigration specialist trained in interviewing and behavioral analysis techniques. Then they meet the young man with the luxuriant hair. The avatar is set up to deliver the standard final set of questions asked of anyone trying to join a trusted-traveler program. Giving their yes-or-no answers to a five-minute robotic catechism, they seem curious or bemused or visibly anxious. One girl, eager to meet the machine after she heard there was a lie detector in the building, behaves as if she's trying her luck on a carnival midway, giddy and excited. On his way out, the old man remarks, "For guys, you might want to make it look like Salma Hayek."

The Nogales field test, intended to reveal the kind of limitations only everyday use can show, has led to further revisions of the kiosk. It's now bilingual, speaking both English and Spanish, and new lab versions have a camera that can collect eye data regardless of the height of the person it's interrogating. Eventually, if the machine flags a traveler as potentially deceptive, that person will be questioned further by a human customs officer. If the traveler triggers no alert, the machine will tell them they're free to go.

When the avatar catches him out, even commissioner Bersin—soon afterward promoted to assistant secretary of international affairs and chief diplomatic officer at DHS—seems to see its potential. He tells a group of customs officers at the DeConcini crossing station that he hopes the kiosk will soon check more and more people coming across the border. "We start off in this more controlled setting, but eventually the payoff is getting it into the lanes," he says.

Customs and Border Protection initially expressed interest in installing five kiosks in each of nine different customs stations, where they would conduct preliminary screening for the Nexus and Sentri programs. Budget issues have now postponed those plans, but last year the research team spent a month showing the machine to several DHS agencies in Washington, DC, including Immigration and Customs Enforcement, TSA, and the Secret Service. Nunamaker, Burgoon, and their colleagues now have funding to research countermeasures and identify the ways people might successfully beat the machine. Meanwhile, the TSA's FAST program, built around Paul Ekman's ideas, has been beset by controversy and technical difficulties. TSA officials now say the agency has no plan to deploy it.

Back in December, the last interviewee of the day at the DeConcini crossing station in Nogales is a stocky Mexican engineer wearing an Otis Elevator ID card around his neck. "So this is the future, huh?" he says at the end of his five-minute interrogation, his face unreadable. "Nice."

It is not yet 5 pm, but it's been a long day of cross-examinations. The customs officer pulls her uniform jacket on over her gun and equipment belt and heads into the rain for home. In the corner of the office, the tech from the university clicks on a wireless mouse a few times. The screen on the Embodied Avatar kiosk flickers, and the device goes to sleep where it stands.

Critical Thinking

1. The researchers in the article say that DHS asked them to study the relationship among emotions, physical cues, and malintent presumably so DHS can predict bad acts before they occur. Do you think this is something we (as a society) should be developing? If we have a tool that can predict malintent and be right most of the time, what should the government do when they find indications of such malintent?
2. The article mentions that Las Vegas casinos use technology to catch cheats. Should private casinos be permitted to evaluate potential cheats with deception detection equipment similar to these avatars? Should retail stores be permitted to evaluate potential shoplifters this way? Should the IRS be permitted to use this during audits? Should a traffic cop be permitted when asking you how much you've had to drink? What general principles should guide acceptable use of deception detection tools?

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

Know Your Rights

Hanni Fakhoury and Nadia Kayyali

Learning Outcomes

After reading this article, you will be able to:

- Articulate the basic principles of the U.S. Constitution Fourth Amendment, and the implications for those principles with the advent of digital communication and storage technologies.
- Understand both the rights and the limitations on search and seizure protections you have under the U.S. Constitution.
- Understand appropriate both legal and behaviors to exhibit if law enforcement requests to search or seize your property in the United States.

Your computer, phone, and other digital devices hold vast amounts of personal information about you and your family. This sensitive data is worth protecting from prying eyes, including those of the government.

The Fourth Amendment to the U.S. Constitution protects you from unreasonable government searches and seizures, and this protection extends to your computer and portable devices. But how does this work in the real world? What should you do if the police or other law enforcement officers show up at your door and want to search your computer?

EFF has designed this guide to help you understand your rights if officers try to search the data stored on your computer or portable electronic device, or seize it for further examination somewhere else. Keep in mind that the Fourth Amendment is the minimum standard, and your specific state may have stronger protections.

Because anything you say can be used against you in a criminal or civil case, before speaking to any law enforcement official, you should consult with an attorney. Remember, generally the fact that you assert your rights cannot legally be used against you in court. You can always state: "I do not want to talk to you or answer any questions without my attorney present." If they continue to ask you questions after that point, you can say: "Please don't ask me any further questions until my attorney is present." And if the police violate your rights and conduct an illegal search, often the evidence they obtain as a result of that search can't be used against you.

We've organized this guide into three sections:

- Overview: When can the police search my devices?
- The police have a warrant. Now what?
- The police can't get into my computer. Now what?

Overview: When can the police search my devices?

- If you consent to a search, the police don't need a warrant.
- Law enforcement may show up at your door. Apart from a few exceptions, police need a warrant to enter your home.
- Be aware that the police can ask your roommate/guest/spouse/partner for access to your computer if they don't have a warrant.
- Even if you're arrested, police can only search your phone under limited circumstances.
- Police can search your computer or portable devices at the border without a warrant.

If you consent to a search, the police don't need a warrant.

The most frequent way police are able to search is by asking you for permission. If you say "yes" and consent to the search, then police don't need a warrant. You can limit the scope of at consent and even revoke or take it back after the officers gin searching, but by then it may be too late.[1] That's why s better not consent to a search—police may drop the mat-. If not, then they will generally need to get a search warrant search.

aw enforcement may show up t your door. Apart from a few xceptions, police need a warrant to nter your home.

e police can't simply enter your home to search it or any ectronic device inside, like a laptop or cell phone, without a arrant.

When the police knock on your door, you do not have to let em in unless they have in their possession and show you a lid search warrant. The safest thing to do is step outside and ut the door behind you. They may or may not indicate right ay why they are there. If they have a warrant, ask to see it. they offer to simply "interview" you, it is better to decline speak until your attorney can be present. You can do this by lling the officer: "I do not want to talk to you. I do not consent a search. I want to speak to my attorney."

There are two major ***exceptions*** to the warrant requirement. rst, if you consent to a search, then the police can search thin the scope of your consent.[2] That's why it is usually bet- to not consent to a search.

Second, if police have probable cause to believe there is criminating evidence in the house or on an electronic device t is under immediate threat of destruction, they can immedi-ely search it without a warrant.[3]

e aware that the police can ask your oommate/guest/spouse/partner for ccess to your computer if they don't ave a warrant.

e rules around who can consent to a search are fuzzy. The y is who has control over an item. Anyone can consent to a rch as long as the officers reasonably believe the third per-n has control over the thing to be searched.[4] However, the lice cannot search if one person with control (for example spouse) consents, but another individual (the other spouse) h control explicitly refuses.[5] It's unclear, however, whether s rule applies to items like a hard drive placed into someone e's computer.[6] And even where two people have control over item or place, police can remove the non-consenting person d return to get the other's consent to search.[7]

You may want to share this know your rights guide with ryone in your home and ask them not to consent to a search law enforcement.

Even if you're arrested, police can only search your phone under limited circumstances.

After a person has been arrested, the police generally may search the items on her person and in her pockets, as well as anything within her immediate control, automatically and without a warrant. But the Supreme Court has ruled that police cannot search the data on a cell phone under this warrant exception.[8] Police can, however, search the physical aspects of the phone (like removing the phone from its case or removing the battery) and in situations where they actually believe evidence on the phone is likely to be immediately destroyed, police can search the cell phone without a warrant.

Police can search your computer or portable devices at the border without a warrant.

Fourth Amendment protection is not as strong at the border as it is in your home or office.[9] This means that law enforcement can inspect your computer or electronic equipment, even if they have no reason to suspect there is anything illegal on it.[10] An international airport, even if many miles from the actual border, is considered the functional equivalent of a border.[11] However, border officials in Alaska, Arizona, California, Guam, Hawaii, Idaho, Montana, Northern Mariana Islands, Oregon and Washington can only confiscate an electronic device and conduct a more thorough "forensic" examination of it if they have reasonable suspicion you've engaged in criminal behavior.[12]

The police have a warrant. Now what?

- Ask to see the warrant.
- The warrant limits what the police can do.
- Although the warrant limits what the police can look for, if they see something illegal while executing a warrant they can take it.
- If the police want to search your computer, it doesn't matter whether you're the subject of their investigation.
- You do not have to assist law enforcement when they are conducting their search.
- You do not have to answer questions while law enforcement is searching.

Ask to see the warrant.

A warrant is a document signed by a judge giving the police permission to either arrest you or search your property and take certain items from that property. You have the right to see the warrant and should check to make sure it is valid.

A warrant should contain:

- The correct name of the person arrested or the correct address of the specific place to be searched;
- A list of the items that can be seized or taken by the police;
- The judge's signature;
- A deadline for when the arrest or search must take place

The police must take the warrant with them when executing it and give you a copy of it.[13] They must also knock and announce their entry before they try to forcefully enter your home,[14] and must serve the warrant during the day in most circumstances.[15]

The warrant limits what the police can do.

The purpose of the warrant is to give the judge, not the police, the discretion to decide what places can be searched and which items can be taken.[16] That's why a warrant is supposed to state exactly what the police can search and seize.[17] However, if the warrant authorizes the police to search for evidence of a particular crime, and such evidence is likely to be found on your computer, some courts have allowed the police to search the computer without a warrant.[18]

And remember, if you consent to a search, it doesn't matter if the police have a warrant; any search is permissible as long as the search is consistent with the scope of your consent.

Although the warrant limits what the police can look for, if they see something illegal while executing a warrant they can take it.

While the police are searching your home, if they observe something in "plain view" that is suspicious or incriminating, they may take it for further examination and can rely on their observation to later get a search warrant.[19] For example, if police see an open laptop with something obviously illegal on the screen, they could seize that laptop.

If the police want to search your computer, it doesn't matter whether you're the subject of their investigation.

It typically doesn't matter whether the police are investigating you, or think there is evidence they want to use against someone else located on your computer. If they have a warrant, if you consent to the search, or they think there is something incriminating on your computer that may be immediately destroyed the police can search it. But remember, regardless of whether you're the subject of an investigation, you can always seek the assistance of the lawyer.

You do not have to assist law enforcement when they are conducting their search.

You do not have to help the police conduct the search. But you should not physically interfere with them, obstruct the search or try to destroy evidence, since that can lead to your arrest. This is true even if the police don't have a warrant and you do not consent to the search, but the police insist on searching anyway. In that instance, do not interfere but write down the names and badge numbers of the officers and immediately call a lawyer.

You do not have to answer questions while law enforcement is searching.

You do not have to answer any questions. In fact, because anything you say can be used against you and other individuals, it is best to say nothing at all other than "I do not want to talk to you. I do not consent to a search. I want to speak to my attorney." However, if you do decide to answer questions, be sure to tell the truth. In many contexts, it is a crime to lie to a police officer and you may find yourself in more trouble for lying to law enforcement than for whatever it was on your computer they wanted.[20]

The police can't get into my computer. Now what?

- The police can take your computer with them and search it somewhere else.
- You do not have to hand over your encryption keys or passwords to law enforcement.
- You may be able to get your computer back if it is taken and searched.
- There is less protection against a search at a place of employment.

The police can take your computer with them and search it somewhere else.

As long as the police have a warrant, they can seize the computer and take it somewhere else to search it more thoroughly. As part of that inspection, the police may make a copy of media or other files stored on your computer.[21]