**Subject:** Fwd: Stranded in (b) (6)
**Date:** Sunday, May 19, 2019 at 11:36:22 AM Eastern Daylight Time
**From:** Yll Bajraktari
**To:** Yll Bajraktari, (b)(6)

Begin forwarded message:

**From:** Eric Schmidt (b) (6)
**Date:** May 19, 2019 at 11:29:54 EDT
**To:** Ylli Bajraktari <(b) (6)>, Robert Work <(b) (6)> Schmidt Support Staff, (b)(6)
**Subject: Stranded in** (b) (6)

Hi there.. sorry to say my airplane is broken and there are no flights tonite that can get me to SFO by the morning; we are working on commercial flights and the plane may be repaired in time

I will keep you posted, but in all cases I will not be there at the beginning

Very sorry but on a Sunday in (b) (6) there are not good alternatives

**Subject:** Re: My messages to NSCAI Email Lists, (b)(6) are bouncing
**Date:** Tuesday, July 2, 2019 at 9:41:58 AM Eastern Daylight Time
**From:** Yll Bajraktari
**To:** Eric Schmidt, Michael Gable, (b)(6)

Will fix it.

On Jul 2, 2019, at 09:39, Eric Schmidt <(b) (6) > wrote:

> Is there a way to get Eric Schmidt, (b)(6) to be able to send to those aliases? Its just much easier for me given my workflow

**Subject:** Re: Beliefs document

**Date:** Saturday, August 3, 2019 at 11:10:40 AM Eastern Daylight Time

**From:** Eric Schmidt

**To:** Yll Bajraktari

**CC:** Robert Work, [redacted], [redacted]

Here are a few comments on the doc and in general

From a friend of mine: "in the west there is increasingly societal reluctance to deploy advanced computing technologies, whereas in China people seem broadly supportive of such advances"
The fact is that some of the most innovative uses of AI will emerge first in China due to lack of regulations and a large and forgiving startup market

On the Four Pillars, at some point you should also mention that the ability to create Synthetic Training data could alter this data balance

Real IA Risks and the Problem of Trust: Basically you should always say that "Because of these issues people will have to supervise these systems"

CHina is investing in Genomics, but I don't agree that the US is not leading in Genomics. Both are investing heavily in Genomics.

I'm not sure that "commercially viable applied research is proceeding at the expense of basic research." What is true is that both are accelerating, and some researchers are being hired to industry but universities are also increasing their basic research capability rapidly.

Foreign talent. What I prefer to say is that we have always had the problem of foreign students in our Universitie and their ability to leak or otherwise transfer that knowledge back to their home countries. The essence of US leadership has been a cost benefit one: the benefit of having the worlds great talent in the US, and the high propensity of them to stay in the US, versus the potential transfer of information to an opponent, has vastly favored the openness of our approach. In other worlds the gains broadly outweigh the losses. You can see this I in the following way: China has lots of talent who are in the US. If they were to stay in China their research would be there, not necessarily open, and they are much more likely to stay in China.
I continue strongly to believe the benefits outweigh the losses. Many of the top graduate students in US universities are foreign born and that is a good thing. We should get all the statistics here and publish them.

"AI is not like a steroid" - A strong statment is that AI is software, and software in procured, specified and built in a way very different from hardware system. The majority of the US government processes do reflect this change and they need to.

There are a few other areas for you to consider :

A) The spread of Generative Networks and GANS in general is an unknown and important development in this area; their ability to be used by nationstate as well as terrorist groups Is unknown but important

B) On semiconductors, the leading firm is TSMC in Taiwan. In the US the leader is Intel. Much of the future depends on large investments in specialized foundries. The US and China have both had concerns about this for decades, and we should say something about this. My personal view is that we need a national disaster plan in case of our overseas Chip supply being cut off. I know that China is also worried about this fo themselves

C) I would say something about the importance of hardware accelerators for AI. They are a new and very important development.

D) I would say something about the potential for new AI algorithms that address the current shortcomings (both fragility and cost). This is something we should be definitive about.

E) I would say something about the potential for Quantum AI, where quantum computing is used to follow the gradient descent algorithms infinitely faster for training.

Thanks !

> On Aug 2, 2019, at 6:14 PM, Yll Bajraktari <(b) (6) > wrote:
>
> Dear Sirs,
>
> Today, I pushed the draft beliefs document to all the Commissioners. NSCAI Staff Members, (b)(6) worked on this document which I believe is a strong foundation for our November report. The document is a great summary of many of the assertions, analysis, and current state of play we have heard during our WGs, plenaries, and meetings with experts.
>
> In my opinion, NSCAI Staff Members, (b)(6) did an outstanding job capturing all the nuances and dynamics related to AI and national security. They wrote the document in a very balanced way, reinforcing our values, our leadership role, and the challenges ahead. I am very pleased with the document and I hope you will have a chance to provide your valuable input.
>
> In addition to the Commissioners, we have shared this document with all our AI experts (NSCAI Special Government Employees, (b)(6) ) as well as our Friends of the Commission (NSCAI Volunteers, (b)(6) ).
>
> I believe that will all the input requested by Sept 1st, we will be in a very good position to start finalizing the November report.
>
> Let us know if there is anything you need from us.
>
> Hope you both have a great month of August and get some well deserved break.
>
> Ylli
> --
> *This message is private and may contain confidential information or other
> matter otherwise protected from disclosure. If you are not the intended
> recipient, please telephone or email the sender and delete this message and
> any attachment from your system; you must not copy or disclose the contents
> of this message or any attachment to any other person. Transmission **of
> any material prepared by a third-party should not be construed to
> constitute an endorsement of that material or any analysis or commentary
> therein by the NSCAI. *

**Subject:** Fwd: Strangelove redux: US experts propose having AI control nuclear weapons - Bulletin of the Atomic Scientists

**Date:** Sunday, September 1, 2019 at 8:30:54 PM Eastern Daylight Time

**From:** Yll Bajraktari

**To:** Yll Bajraktari, (b)(6)

Begin forwarded message:

**From:** Eric Schmidt <(b) (6)>
**Date:** September 1, 2019 at 20:14:17 EDT
**To:** Yll Bajraktari, (b)(6), Robert Work, (b)(6)
**Subject: Strangelove redux: US experts propose having AI control nuclear weapons - Bulletin of the Atomic Scientists**

Strangelove redux: US experts propose having AI control nuclear weapons - Bulletin of the Atomic Scientists

https://thebulletin.org/2019/08/strangelove-redux-us-experts-propose-having-ai-control-nuclear-weapons/

**Subject:** Re: We Need to Prepare for the Future of War
**Date:** Tuesday, September 10, 2019 at 1:51:10 PM Eastern Daylight Time
**From:** Eric Schmidt
**To:** Yll Bajraktari
**CC:** Robert Work

yes very very good and surveys everything well

On Sep 10, 2019, at 10:53 AM, Yll Bajraktari <(b) (6) > wrote:

Good article.

https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html?action=click&module=Opinion&pgtype=Homepage

Opinion



# N.S.A. Official: We Need to Prepare for the Future of War

Technology is about to upend our entire national security infrastructure.

**By Glenn S. Gerstell**

Mr. Gerstell is the general counsel of the National Security Agency.

- Sept. 10, 2019

The National Security Operations Center occupies a large windowless room, bathed in blue light, on the third floor of the National Security Agency's headquarters outside of Washington. For the past 46 years, around the clock without a single interruption, a team of senior military and intelligence officials has staffed this national security nerve center.

The center's senior operations officer is surrounded by glowing high-definition monitors showing information about things like Pentagon computer networks, military and civilian air traffic in the Middle East and video feeds from drones in Afghanistan. The officer is authorized to notify the president any time of the day or night of a critical threat.

Just down a staircase outside the operations center is the Defense Special Missile and Aeronautics Center, which keeps track of missile and satellite launches by China, North Korea, Russia, Iran and other countries. If North Korea was ever to launch an intercontinental ballistic missile toward Los Angeles, those keeping watch might have half an hour or more between the time of detection to the time the missile would land at the target. At least in theory, that is enough time to alert the operations center two floors above and alert the military to shoot down the missile.

But these early-warning centers have no ability to issue a warning to the president that would stop a cyberattack that takes down a regional or national power grid or to intercept a hypersonic cruise missile launched from Russia or China. The cyberattack can be detected only upon occurrence, and the hypersonic missile, only seconds or at best minutes before attack. And even if we could detect a missile flying at low altitudes at 20 times the speed of sound, we have no way of stopping it.

The threats of cyberattack and hypersonic missiles are two examples of easily foreseeable challenges to our national security posed by rapidly developing technology. It is by no means certain that we will be able to cope with those two threats, let alone the even more complicated and unknown challenges presented by the general onrush of technology — the digital revolution or so-called Fourth Industrial Revolution — that will be our future for the next few decades.

The digital revolution has urgent and profound implications for our federal national security agencies. It is almost impossible to overstate the challenges. If anything, we run the risk of thinking too conventionally about the future. The short period of time our nation has to prepare for the effects of this revolution is already upon us, and it could not come at a more perilous and complicated time for the National Security Agency, Central Intelligence Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation and the other components of the intelligence community.

> The immediacy and specificity of the war on terror following the Sept. 11 attacks permitted the intelligence community to reorient itself relatively quickly and effectively from the Cold War and its immediate aftermath. But the intelligence community and its allies who rely on one another for information-sharing must now adapt to adversaries with new capabilities — principally China, Russia, Iran and North Korea, each of which presents different and complex threats — while still not forsaking the counterterrorism mission.

Gearing up to deal with those new adversaries, which do not necessarily present merely conventional military threats, is itself a daunting challenge and one that must be undertaken immediately and for at least the next decade or two. But that is precisely when we must put in place a new foundation for dealing with the even more profound and enduring implications of the digital revolution.

That revolution will sweep through all aspects of our society so powerfully that our only chance of effectively grappling with its consequences will lie in taking bold steps in the relatively near term. In short, our attention must turn to a far more complex set of threats of multiple dimensions enabled by the digital revolution. While the potential consequences are less catastrophic than nuclear war, they are nonetheless deeply threatening in a range of ways we will have trouble countering.

There are four key implications of this revolution that policymakers in the national security sector will need to address:

The first is that the unprecedented scale and pace of technological change will outstrip our ability to effectively adapt to it. Second, we will be in a world of ceaseless and pervasive cyberinsecurity and cyberconflict against nation-states, businesses and individuals. Third, the flood of data about human and machine activity will put such extraordinary economic and political power in the hands of the private sector that it will transform the fundamental relationship, at least in the Western world, between government and the private sector. Finally, and perhaps most ominously, the digital revolution has the potential for a pernicious effect on the very legitimacy and thus stability of our governmental and societal structures.

What I offer here is more of a sketch than a finished painting; our national policymakers and the future leaders of those agencies will be responsible for addressing these foreseeable challenges and ultimately finding solutions.

While these trends have been extensively discussed in the press, academia and the technical world, there has been far less attention devoted to understanding the combined effect the trends will have on the various agencies that help keep our nation safe. I hope to rectify that shortfall.

We all sense that we are on the cusp of unimaginable technological changes. Cellphones and the internet seem of such manifest utility that we take them for granted, but that is only because they have become so central to our daily lives, not because they have been around forever. Indeed, as we are often reminded, Google started in 1998. YouTube is only 14 years old, and the iPhone is merely 12 years old. The digital revolution thus far is distinguished by its ability to become ubiquitous in our daily personal and commercial lives in an astonishingly rapid time, a time frame that is really without precedent.

Other transformational technologies, such as railroads, electricity, radio, television, automobiles and airplanes, all took several decades before they reached that comparable level of ubiquity. Society had the time to sort out the norms, rules and laws governing those technologies and the respective roles of government and the private sector. Consider, for example, the lag between the advent of the first useful automobile in the late 19th century and the late 1960s, when safety features became truly significant and mandatory. By contrast, today, just a dozen years after Facebook became a "thing" in our lives, we are forced to grapple with whether and how we should regulate hateful postings and mendacious foreign electoral influence on social media platforms.

Facial recognition technology has in just a handful of years become sufficiently accurate as to be useful and thus more common, but its persistent imperfections have led to a confused spate of lawsuits and statutes seeking to regulate its use. We are far from figuring out its proper role in our society. So the windows for how long it takes for technology to shape society and — more pertinent to this discussion — how long it takes for us to sort out the associated challenges are becoming almost impossibly compressed.

The time compression for our society and ultimately our national security agencies to deal with these challenges is

> but one aspect of the problem. The sheer amount of data that will be generated by individual and commercial activities, with the Internet of Things and 5G cellular connectivity, is incomprehensible and will require entirely new ways of rendering that data meaningful to agencies whose mission is to discern threats to national security.

We will need new technologies and systems to capture, analyze and store this data. Obviously, that will require enormous investments by the United States and its allies to upgrade national security and surveillance systems. Will Western liberal democracies, already straining under the combined demands of decaying civil infrastructure, aging populations, upgrading militaries and so on, be able to afford these investments? Given that there is no specific forcing event to require greater resources, but rather a trend, history suggests that we will appreciate the seriousness of the underinvestment only when a crisis has occurred.

That approach might be a barely acceptable way for our society and government to address social ills and decaying infrastructure, which are slower-moving problems, where with enough resources one might catch up. But the same approach could well be disastrous when addressing rapidly evolving technological matters, especially where national security is at stake. Without such investments, our national security agencies risk becoming profoundly less effective or marginalized.

> While extraordinary levels of new investment will be required to deal with the sheer quantity of data, that alone will not be sufficient. It is futile to believe that we will be able to spend our way to success. Rather, we will need to couple large investment with entirely new ways of approaching how we collect, manage and make sense of this data. One key aspect of any such new approach will be a heavy reliance on machine learning and artificial intelligence. We thought wrestling with the challenges of the Fourth Amendment in addressing electronic surveillance over the past few decades was complicated and contentious, but

setting norms for A.I. will surely be even more fraught with difficulty. The stakes are much higher, given that A.I. will be intrinsic to determinations and decisions of almost every aspect of our personal, professional and commercial lives. A.I. opens up the possibility of rendering intelligible for national security purposes that ocean of data. But if misused or even if not thoroughly understood, A.I. can yield nefarious and corrupting results for our society.

Since A.I. is still relatively nascent, our surveillance and analytic resources are not well positioned to deeply understand how adversaries might be using it in the future. The range of novel issues is daunting. For example, we will need to understand how to defend our analytic systems against data poisoning, in which an adversary can feed misinformation to A.I. systems to corrupt or defeat them (such as causing a driverless car to ignore a stop sign).

We will also need to understand the protocols by which future autonomous weapons — drones, tanks, armed robots — will be controlled so that we can defend ourselves. Will the availability of huge numbers of nonhuman war-fighting machines increase the chances of war, as policymakers might be more willing to sacrifice those machines than humans? Or will such machines permit some not-yet-conceived lower threshold of machine-to-machine conflict — whether involving cyber or physical machines — that does not rise to the level of a full-fledged war? Our national security agencies will require new experts and resources to understand the intentions and capabilities of adversaries in this new and developing area.

Understanding the promise and threat of quantum computing will also require vast expansion of our expertise in this extraordinarily sophisticated area. It is true that no one has yet built a functioning quantum computer. Perhaps no one ever will. But it seems more likely than not that before the middle of this century either China or the United States will do so, with extraordinary advantages for whichever nation gets there first.

Unlike the electronic digital computers we have used for

over a half century, quantum computers are based on a fundamentally different concept, relying not on simple "on" and "off" states of electricity but on the complex properties of atomic and subatomic particles. One strategic benefit is that quantum computing will enable something that even our current supercomputers cannot do — crack strong encryption of the type that now protects our commercial financial transactions, our weapons systems and government's secret communications. China's publicly announced 2030 goal is to develop a high-performing quantum computer, which should have that decryption ability. Imagine the havoc that could create. Imagine the overwhelming leverage that the winner would have — such a decryption ability could render the military capabilities of the loser almost irrelevant and its economy overturned.

The analogy of the postwar world in which there was only one nuclear power hints at the type of unilateral dominance that might be possible for the quantum computing victor — but it is not apt here. Even with a nuclear monopoly, there were very real limits on utilizing that capability. But not so with the unilateral capability to decrypt — and thus to understand and perhaps to interfere with or destroy — the entire digital existence of an adversary country.

The strategic advantage here would be for one country to surreptitiously acquire such a capability and maintain it for perhaps several years or more. Other countries would not realize that everything from their weapons systems to financial transactions would be vulnerable during that period; and that would include not only current activity but also the historic, encrypted communications collected and retained by the winner in anticipation of this very capability.

Indeed, one of the strategies yet to be developed involves the paradox of how a country with such capability could exploit it without revealing the capability's existence. Moreover,

> shifting to quantum-resistant algorithms and encryption is theoretical and thus uncertain, but will surely be expensive and a decades-long endeavor.

Over the past several decades, the intelligence community has built up an extraordinary capability to understand the military doctrines and weapons systems of Russia and China. That will still be relevant, but there is now a fundamentally new additional requirement. Under the best of circumstances, it would take many years to develop comparable levels of expertise about those countries' use of A.I., quantum computing or other novel technologies. Such technologies range from hypersonic missiles, which Russia and China are racing to develop — with the potential to upend the entire global balance of power — to synthetic biology and genetic manipulation, with the potential to create new biological weapons or immunities. Our national security sector does not have an extensive history of marrying intelligence insight and analysis with deep technical expertise across a wide range of scientific disciplines.

That might not, however, be the limiting factor.

> It is by no means assured that our national security sector will be able to attract on a sufficient scale the scarce engineering, mathematical and scientific talent that would supply the necessary expertise. That challenge will require investment, enlightened strategic management and an innovative approach to luring a different type of expert out of the private sector into government. Meeting this challenge will require a greater reliance in general on the private sector, since government alone does not possess the requisite expertise. A large portion of the intelligence community's experts on the military capabilities and plans of Russia and China joined government during the Reagan administration; other experts on counterterrorism and new technology burnished their technical skills following the Sept. 11 attacks. Many of those experts are nearing

retirement or have already left to join an attractive private sector. With millennials believing that technology in the private sector now allows them to help change the world — previously the idea of a mission had been largely the province of public service — it is not clear that the intelligence community will be able to attract and retain the necessary talent needed to make sense of how our adversaries will make use of the new technology.

In short, while important work has been done in examining and laying the foundations for the critical role new technologies will play in national security, much more needs to be done. We must ask whether our defense and national security establishments are in a position — financial and technical — to succeed in these critical technologies that could either solidify our continued position as the leading global power or reduce us to a clearly subordinate role. We are talking about national initiatives that collectively will dwarf the effort to put a man on the moon.

Bluntly put, there are few signs that our society overall and our political leaders have fully embraced the challenge or appreciate the risks of failure.

All of this technological innovation will surely bring significant societal benefits, perhaps most notably in the area of health care and genetic engineering, but it will also increase — to use a hackneyed but useful term — the "attack surface" for cyber mischief. This takes us to the second implication of the digital revolution: We must prepare for a world of incessant, relentless and omnipresent cyberconflict — in not only our national security and defense systems (where we are already used to that conflict) but also, more significantly, every aspect of our daily and commercial lives.

The sensors, systems, networks, algorithms and machines that will empower our new lives — whether health care implants, driverless cars, pilotless aircraft or food safety protections — will all be part of the Internet of Things. One consequence is that the current division between

> cyberdefense (think firewalls, penetration testing and cyberhygiene) and supply-chain risk management (think of the assessment of equipment manufacturing, component assurance and availability and surveillance concerns in equipment) will be eliminated, with everyone concerned with the holistic sanctity of equipment and software to achieve the well-recognized triad of availability, security and integrity.

The 40-odd nation-states that today have offensive cybercapabilities will seem a quaint historic artifact when sophisticated tools for cybermischief are in the hands of not only every nation-state but also common criminals around the globe. While most nation-states might be careful to limit their cybereffects to economic theft and espionage, pre-battle positioning of beacons and other malware, mischievous interference with elections and public opinion — all below levels that cause significant physical damage to infrastructure or physical harm to humans, and thus below at least what we currently think of as the threshold for an act of war — there is no guarantee that all nations will exercise such care nor that criminals would be deterred. Consider how North Korea seems able to operate with relative impunity in cyberspace, knowing that it is unlikely to provoke an armed attack partly because of its perceived willingness to retaliate in ways that would impose unacceptable consequences on Western society. Multiply that dynamic across a dozen or more countries or international terrorists or criminal gangs and we are now faced with an entirely different national security threat.

To be sure, our nation has set forth its cyberstrategies and continues to refine its offensive and defensive doctrines in cyberspace, but nearly every expert would concede more needs to be done. The question is whether we will be able to do it in time, since the threat is coming at us with the speed and force of a tsunami.

> The simple fact of the matter is that no nation has yet devised an effective solution to the conundrum of how to

> respond in a definitive and dispositive way to another nation-state's malicious cyberactivity. Whole-of-government approaches — economic sanctions, judicial prosecutions and offensive cyberresponse below the war threshold — while essential and appropriate, have not been enough to stop cybermalevolence. In short, the problem is going to get worse before it gets better.

In all probability, it will get better not because we develop more effective deterrents (although threats of cyberretaliation and imposition of other burdens clearly do play a key role here, at least with other nation-states) but because we develop greater resilience and more impervious defenses — and the full realization of that may be a decade away.

In the meantime, our national security agencies will be confronted with the political imperatives in our democracies of responding (at least in some way) to cyberthreats. Among other things, our citizens and businesses will have to accept that cybermalevolence is a persistent threat, not a war to be won or a disease to be cured. Moreover, since the threat is ignorant of sovereign boundaries, agencies charged with cyberprotection will be required to work with many others around the globe, perhaps including those of adversary or competitor nations, creating new complexities.

> At a minimum, the worldwide cyberthreat will put a premium on trusted relations among the Five Eyes (the United States, Britain, Canada, Australia and New Zealand) and other like-minded nations, to facilitate working together to counteract malevolent activity that can span the globe in seconds. Even among such long-term, cohesive arrangements as the Five Eyes alliance, unity of effort in cyberspace is not assured, as witnessed recently by differing approaches to the risks posed by Huawei equipment in 5G networks.

The third implication of the digital revolution is that the balance between government and the private sector will be altered in a profound way. That in turn is the inescapable product of three factors: cybervulnerability affecting every element of the private sector (no longer are targets arguably limited to military assets), the general flood of data unleashed by the digital revolution that will be created in the hands of private enterprise and a response to a rising China whose strategic technology goals pose a unique threat that directly implicates the private sector.

Even without considering the challenges presented by China, there are at least two, related manifestations of how the government-private sector balance has changed and will change. First, the government no longer possesses the lead in complex technology, at least in many areas relevant to national security. Arguably, the most powerful computing and sophisticated algorithm development now occurs not in the Pentagon or the N.S.A. but in university research labs and in the Googles and Amazons of the commercial world. (To be sure, the government still maintains its superiority in important areas ranging from nuclear energy to cryptography.) Even apart from the issue of which sector has the technological edge, there is the simple fact that the digital revolution has brought astonishing capabilities to anyone who has a smartphone, who can now download a facial recognition app, a malicious cybertool or some other capability that formerly was the exclusive province of government.

Second, the private sector will have many more times the quantity of data about individuals and commercial activity than governments could ever obtain. The larger antivirus vendors, with their sensors connected to their global corporate clients, already know more at any given moment about the state of networks around the world than does any government agency. Businesses in the services, retailing, industrial and other sectors will have more global sensors and applications detecting cybertraffic, collecting behavioral

patterns, amassing personal data and so on, than even the most surveillance-oriented nation could ever hope to have. The fact that private satellite imagery companies have displaced the monopoly that the National Geospatial-Intelligence Agency used to have is merely a harbinger of how the private sector will be the collector and repository of key information about our locations, our consumption patterns, our communications — in short, about everything.

As the owners of physical infrastructure learned following the Sept. 11 terrorist attacks, when our everyday lives rely on the security of assets and services held in the private sector, commercial owners will be expected to take steps to protect society. We are clearly witnessing the same imbuing of social responsibility into how the digital revolution's data will be handled. Personal data needs to be safeguarded so that it does not fall into the wrong hands, it needs to be made accurate so that incorrect results are not generated from its use, and it needs to be used in ways that do not violate our notions of privacy and proper use. Those are not duties originating within the commercial world but will be increasingly imposed by society.

As for the safeguarding, many would argue that governments cannot and should not be relied on to prevent and defend against every cyberthreat to the private sector, even from a nation-state; such threats are not the same as an armed attack. But that leaves the private sector frustrated and underdefended — hacking back is often impossible and generally illegal.

National security agencies will need to defuse that frustration and find an effective path for collaboration with the private sector to mitigate cyberthreats. The only practical solution is for the private sector to assume a greater burden in this area, but with the active support of the national security agencies. We are still struggling to find

> an effective solution to the competing desires for the private sector to obtain classified information about cyberthreats and for government to obtain detailed information about cyberintrusions into corporate networks. Both sides have legitimate reasons to keep their information secret. But ultimately we all realize that will not yield an effective outcome. Attribution solutions will require the private sector to be more forthcoming about network breaches. Indeed, the private sector should have a greater responsibility to collect, analyze and retain all this new data and to make it available with appropriate safeguards to the government for national security purposes. But even safeguards will not completely allay a variety of privacy and liability concerns.

Until recently, at least in the United States, our notions of privacy have been rooted in the Fourth Amendment's delineation of the federal government's powers vis-à-vis the individual citizen. But what do our notions of privacy mean anymore when Amazon, Google, Apple, Microsoft, Facebook and so on already know so much about you? We now see increasing pressure in Congress to regulate in this area. To be sure, this article is not advocating any particular approach (much less suggesting greater surveillance powers), but it is hard to escape the conclusion that we will need to recalibrate the balance in this area of data privacy between the government and the private sector.



National security agencies should affirmatively contribute to the public discourse about this recalibration. The challenge for those agencies will be to find the right approach to working with the private sector to obtain the data needed to fulfill their vital missions in a manner that fits our values and cultures.

Of course, there is another path, and it is the one taken by authoritarian regimes around the world. China's approach is to have all that data

reside in the central government, in a vast databank of personally identifying information about its citizens, from iris and facial recognition to DNA data. That is antithetical to our values.

> But it is equally true that to keep our society safe, those charged with that mission will need some access to that data. Absent some satisfactory calibration, our national security agencies run the risk of being marginalized and ultimately irrelevant and ineffectual, with grave consequences for national security.
>
> Eschewing the approach taken by authoritarian regimes to data collection and usage by no means reveals the proper path to be taken, as any decision would be deeply linked to the historic roles of government and the private sector in each country. The approach in Western Europe, with close cooperation between public and private sectors, might seem inappropriate if not impossible in America.
>
> For two examples, consider the integrated cybercenters in Britain and the level of government involvement in private sector data usage under the European Union's General Data Protection Regulation. Would the American business community accept that model, and would our national politics permit its adoption? Paradoxically, the global cyberthreat and the overall challenges presented by the digital revolution may propel national security agencies of many countries to work together, but they may find closer cooperation difficult in practice as the balance between public and private sectors will vary greatly from nation to nation.

Finally, our nation will have no choice but to harness the collective capabilities of the government and the private sector to address the combined technologic and economic threats posed by China. For the first time since the United States became a global power, it must now confront an adversary that presents not merely a political or military threat but also an

existential economic one. But in the latter area, the playing field is not level, as China advances its national strategic goals through a unified effort harnessing its government and its business sectors (the latter being a mix of private and state-sponsored endeavors) — while our strategic goals are seen as the responsibility of the federal government, with our private sector largely free to pursue its capitalist interests as it sees fit.

The almost inescapable fact that China's economy will surpass ours in size has obvious national security implications. But two circumstances present special challenges for our national security community. The obvious one is that China continues to seek economic and military superiority through cybertheft from our government, defense industrial base and academia. The second is that our national security agencies for the first time must amass the talent and systems to understand not simply a military challenge but also challenges across a broad range of technology and global finance issues. The capacity for such understanding currently resides principally in the private sector and our universities, not the federal government.

Both of those circumstances will force the government and private sector to work together in unprecedented coordinated and mutually supportive ways if we are to rise to the challenges posed by China. That will require changes in not only attitudes (on both sides) but also laws to permit greater collaboration.

The digital revolution is at least partly responsible for another disruptive effect on the relationship between governments and the private sector, namely the almost complete globalization of economic forces. That capital is now a global commodity shows the relative shortcomings of a nationalistic approach to protect vital assets. Most Western democracies have some rules to regulate foreign investment in critical industrial sectors. In the United States, the Chinese have figured out that it is easy to sidestep the strictures of the Committee on Foreign Investment in the United States, which limits foreign investment in nationally sensitive industries, simply by

> investing in start-ups and other ventures that have access or insight into critical technologies or by working in university research labs to the same end. This may well be another factor weakening the role of nation-states in providing security and tilting the balance of power toward the private sector, which is in a better position to police unwanted investments and intellectual property theft.

As if all this is not disconcerting enough, the fourth implication is that the internet can have a pernicious effect on our democracies, where adversaries can take advantage of our freedoms and interfere with our societal and government institutions. The painfully obvious fact is that the internet affords everyone a communications capability. In the absence of a commonly accepted authority — whether it be a trusted government or a curated news source — the internet permits lies and evil to be spread with almost no check.

> A world in which effective deception in almost every venue and media outlet is possible vastly complicates the duties of government and societal institutions. Even if a nation were to control its own citizens' activities, information (whether accurate or not) knows no national boundaries.

We all recognize this decentralizing and delegitimizing force, and there is no need to elaborate on it here. Worth appreciating in this context, however, is that governmental agencies with a national security mission are going to find it vastly more difficult to maintain the necessary trust, respect and support of a democratic populace in this environment — jeopardizing not only their ability to obtain resources from society but also in the end their very mission.

Indeed, the state of affairs of fundamental uncertainty and doubt that will be facilitated by the misuse of digital technology may well make it more difficult to maintain foreign alliances (which, after all, are based on trust) — precisely at a time, paradoxically, when global cooperation is required to counter malicious activity. In short, and perhaps most critical to appreciate, the fourth implication of the digital revolution is that it will make dealing with the first three implications all the more problematic.

Putting these four implications together — coping with unprecedented technological change, adapting to a world of unceasing cyberconflict, navigating concepts of privacy and the power that comes with access to big data in the hands of the private sector, and countering the insidious and pernicious effects of the delegitimization afforded by the malign use of the internet — yields at least two imperatives, both of which are transformational.

The first imperative is that our national security agencies must quickly accept this forthcoming reality and embrace the need for significant changes to address these challenges. This will have to be done in short order, since the digital revolution's pace will soon outstrip our ability to deal with it, and it will have to be done at a time when our national security agencies are confronted with complex new geopolitical threats.

Much of what needs to be done is easy to see — developing the requisite new technologies and attracting and retaining the expertise needed for that forthcoming reality. What is difficult is executing the solution to those challenges, most notably including whether our nation has the resources and political will to effect that solution. The roughly $60 billion our nation spends annually on the intelligence community might have to be significantly increased during a time of intense competition over the federal budget. Even if the amount is indeed so increased, spending additional vast sums to meet the challenges in an effective way will be a daunting undertaking. Fortunately, the same digital revolution that presents these novel challenges also sometimes provides the new tools (A.I., for example) to deal with them.

The second imperative is we must adapt to the unavoidable conclusion that the fundamental relationship between government and the private sector will be greatly altered. The national security agencies must have a vital role in reshaping that balance if they are to succeed in their mission

to protect our democracy and keep our citizens safe. While there will be good reasons to increase the resources devoted to the intelligence community, other factors will suggest that an increasing portion of the mission should be handled by the private sector. In short, addressing the challenges will not necessarily mean that the national security sector will become massively large, with the associated risks of inefficiency, insufficient coordination and excessively intrusive surveillance and data retention.

A smarter approach would be to recognize that as the capabilities of the private sector increase, the scope of activities of the national security agencies could become significantly more focused, undertaking only those activities in which government either has a recognized advantage or must be the only actor. A greater burden would then be borne by the private sector.

For example, our society could consider greater coordination between government and the private sector in advancing national security strategic goals (such as development of quantum computing capabilities), specific requirements for the private sector to share (with appropriate safeguards) proprietary data and technology with the government where directly relevant to national security, or a duty to notify government of the details of cyberincidents. Perhaps we should rekindle the discussion over a national service obligation to help supply technical expertise to the government across a broad range of fields, or otherwise create some arrangement to make such expertise available to government (rather than the current model in which the private sector often lures away government-trained talent). The point here is not to advocate for any of these, simply to say our policymakers need to be examining alternatives if we are to close the forthcoming technology gap.

Although I have sketched out some of the more troublesome implications of the digital revolution for the national security sector, it is not in the spirit of forecasting doom, but rather to sound an alarm.

Our innovative and entrepreneurial society affords us a unique advantage in dealing with those implications.

Moreover, no adversary should ever underestimate the extraordinary capabilities of our armed forces and intelligence community — like those keeping watch at the National Security Operations Center. Their prowess and resilience will be key in addressing future challenges. But it would be a mistake to rely on these strengths alone.

Surmounting the transformational challenges posed by this Fourth Industrial Revolution will require not merely resources and creativity from both the public and private sectors but also, and more critically, a level of concerted national political will that may be made all the more difficult to achieve by the very attributes of the digital revolution rushing toward us.

Mr. Gerstell is the general counsel of the National Security Agency and previously served as a member of the president's National Infrastructure Advisory Council.

# General Purpose Talking Points

**THE COMPETITION:** The U.S. is in a geopolitical competition, with technology at the center. American security and prosperity hinges on the competitiveness of our economy, and our ability to defend our interests with military power.

- Competitive military advantage depends on an innovative and responsive industrial base with AI at the center.
- China believes AI will let them compete more equally with, if not surpass, the United States in both economic and military power.
- **The Imperative:** Extending U.S. leadership in all aspects of AI from research to application is a strategic, economic, and ethical imperative.

**WHY U.S. LEADERSHIP MATTERS**: US leadership enabled the West to thrive, and provided stability in Asia that also allowed China to rise over the last 40 years. Now China and Russia are challenging this paradigm.

- The country at the forefront of AI will have the greatest capacity to shape a world consistent with its interests and values. We must be the leaders in setting rules/norms for AI ethics and application. This hinges on U.S. retaining technical leadership, while developing **a national consensus on the Ethics of AI.**
- The U.S. can better compete with data-rich strategic competitors in AI by expanding the data pool to include allies and partners. Potential for **better and improved coordination with allies and partners** to develop a larger network focused on data sharing. **We need to treat data as a strategic asset.**

**WHAT WE MUST DO**:

- **More R&D investment in AI.** Commercial investment in R&D dwarf U.S. government investments. Markets incentivize near-term applications. Federally-sponsored and conducted R&D provide a critical foundation for basic research. We need both to stay competitive for the long game. Current federal funding is inadequate for the challenge.
- It is time to **refresh the American public-private relationship** based on a shared sense of responsibility. The federal government must reinvigorate trust through transparency, while industry must help tackle the challenges AI poses for society and security. Protecting our shared values and principles is central to sustain America's innovative edge.
- **Accelerated AI adoption and application** is required to sustain the U.S. advantage in defense and intelligence. "Without some type of unified, DoD-wide adoption of an AI foundation, the Department will soon reach a tipping point after which it will be unable to catch up to its competitors."
- **More investment in people and tech in national security and defense is crucial to overcome the adoption obstacles.** We must **change how we recruit, retain, and incentivize talent.** We also **need institutional and organizational changes, and potentially new AI-specific agencies and technology-specific academies**.
- AI talent now flows from China to the U.S. This needs to be preserved. Options to keep talent flowing to America through laws and incentives need to be expanded so the country will continue to benefit from **high skilled immigration – need to remain a magnet for the world's best.**
- **Advances in AI depend on progress in computing**. Public-private partnership is required to ensure advanced computing technology at scale while simultaneously funding research and investment in future technologies necessary to run advanced AI algorithms.

**Subject:** Fwd: 2021 Thoughts
**Date:** Wednesday, September 11, 2019 at 5:59:26 PM Eastern Daylight Time
**From:** on behalf of Yll Bajraktari
**To:** NSCAI Staff, (b)(6)
**Attachments:** General Talking Points Sept 9 2019.docx, ATT00002.bin

Team,

Thanks for everyone in helping with this document.

Eric liked the document and wants to add two things which I think are good.

Best, Ylli

Begin forwarded message:

> **From:** Eric Schmidt <(b) (6)>
> **Date:** September 11, 2019 at 17:53:09 EDT
> **To:** Yll Bajraktari, (b)(6)
> **Cc:** Robert Work <(b) (6)>
> **Subject: Re: 2021 Thoughts**
>
> THis is good thank you
>
> I would revise and add something about specific areas:
>
> For example, our Intelligence services need to be completely reimagined in the era of infinite information
> For example our military strategies have to be completely reimagined in a world of zero time to react and artificial intelligence pushing the offensive attack
>
> There must be a few pithy and interesting points in this area..
>
> > On Sep 8, 2019, at 9:27 PM, Yll Bajraktari <(b) (6)> wrote:
> >
> > <General Talking Points Sept 9 2019.docx>

**Subject:** Fwd: Really good
**Date:** Wednesday, September 11, 2019 at 12:46:22 PM Eastern Daylight Time
**From:** on behalf of Yll Bajraktari
**To:** NSCAI Staff, (b)(6)

I shared this earlier but good to know that Eric liked it too.

Begin forwarded message:

> **From:** Eric Schmidt <(b) (6) >
> **Date:** September 11, 2019 at 12:30:57 EDT
> **To:** Yll Bajraktari, (b)(6), Robert Work, (b)(6)
> **Subject: Really good**
>
> U.S. Intelligence Needs Another Reinvention - The Atlantic
>
> https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/