



[[remember to start recorder!!]]

Thanks to Uli and Max, and STS Dept

Word of note: I'm using common usage of "technology" in sense of products in this talk, rather than in the sense understood in export controls as 'Specific information necessary for the "development", "production" or "use" of a product.'

We are at potential inflection point in how conceive and govern security concerns in science and technology, particularly in areas like computing and biology.

My argument is that the nature of this inflection point turns not on areas of science and technology where there is wide agreement on

- WHO we are worried about
- WHAT S&T we don't want them to get because we think using it will cause illegitimate harm
- Who the WE is, e.g. the state

INSTEAD: The area where I think change is needed is specifically in the ways we think about and govern security concerns when

- The thing to be governed is ambiguous
- it's not clear who has the authority to decide
- nor is it clear what should be done if we are concerned.

For most of history, we've not paid much attention to studying this grey zone.

I'll take you through a set of examples of how these questions have been answered in the past, and the troubles we're seeing with them today.

If we look at how security concerns around S&T are discussed in the media, we quickly discover a pattern:

The collage features three distinct sections:

- Left Section (STAT):** A snippet from a STAT article titled "Biohackers are about open-access to science, not DIY pandemics. Stop misrepresenting us" by Daniel Grushkin, dated June 4, 2018. It includes a photo of a group of people in a lab setting and a caption: "A class at GenSpace, a community lab in Brooklyn."
- Center Section:** A large, bold text graphic that reads "Are we too concerned or not enough?" with "Bioengineering" written below it.
- Right Section (Business Insider):** A snippet from a Business Insider article titled "Bill Gates thinks a coming disease could kill 30 million people within 6 months – and says we should prepare for it as we do for war". It features a photo of Bill Gates and a list of bullet points:
 - The next deadly disease that will cause a global pandemic is coming, Bill Gates said on Friday at a discussion of epidemics.
 - We're not ready.
 - An illness like the pandemic 1918 influenza could kill 30 million people within six months, Gates said, adding that the next disease might not even be a flu, but something we've never seen.
 - The world should prepare as it does for war, Gates said.

The debate is often framed around either being too concerned about security concerns around an area of science and technology, or that we are not concerned enough.

Too concerned: security concerns hinder innovation (Grushkin)

Not concerned enough: Global pandemic from bioterror (Gates)

CHATHAM HOUSE


Home > Experts > Expert Comment >

Banning Autonomous Weapons Is Not the Answer

In this section

2 May 2018

A simple ban of lethal autonomous systems, as advocated for by some states, misses the complexity of the issue and how highly-automated systems could actually enhance adherence to international law.


 Major Kathleen McKendrick

Are we too concerned or not enough?

Computing

The New York Times

How a Pentagon Contract Became an Identity Crisis for Google



Mark Long/The New York Times

By Scott Shane, Cole Metz and Daijike Wakabayashi
May 30, 2018

WASHINGTON — Fei-Fei Li is among the brightest stars in the burgeoning field of artificial intelligence. Somehow managing to

Sam Weiss Evans 3

Too concerned:

Not concerned enough: Google DoD



- Deep history of a) governing security concerns in technology, b) secrecy and c) the concept of academic freedom
- Attempts to govern S&T of ambiguous security concern in 20th C
- Current efforts to rethink the governance of security concerns in science and technology

Outline

Deep history of

- a) governing security concerns in technology
- b) secrecy
- c) the concept of academic freedom

Sam Weiss Evans 5

When most people place the beginning of modern systems to govern security concerns in S&T, they usually peg the early to mid-20th Century.

League of nations

nuclear weapons

secrecy controls on science ala Atomic Energy Act

But it's worth going much further back, because the assumptions that all those systems were grounded on a deeper history of the how to govern security concerns in science and technology and who should do the governing, as well as the separate histories of secret communication and the role of science, and in particular Universities, in society.

This means there are deeply seated ways that we have to see what should count as a threat in S&T, and what to do about it, and who is responsible.

So in this section, I'll be bringing us from hundreds of years ago up until about WWII on each of these histories, then we'll take it from there in the next section.

Basic assumptions of many S&T security governance mechanisms

- Run by states
- Clearly defined objects (excludable)
- Lists of objects change slowly
- Known enemy (outside of state)
- Clear state boundaries over which trade can be monitored

Sam Weiss Evans 6

There are many instances where this way of thinking still is very important: the means of war at a state level is something we would all like to keep an eye on
Let's take the example of export controls



Restricting trade in militarily useful items has a very long history

Aristophanes

– it was never JUST military items, but also things that had multiple uses

The Pope in the 12–13thC decreed that not only arms, but also shipbuilding supplies and wood should be restricted in trade with the “Saracens”

By the time the concept of the modern state was forming in 17C Europe, this was the scene where technology was thought to be controlled.

- tangible goods
- seaport (or at least by ship)

Hugo Grotius just wrote down the common division of goods at the time

- Absolute contraband
- Conditional contraband: depends on who is going to.
- Free

Grotius didn't himself write down an actual list of items (wisely), but when states went to war, they regularly posted lists of absolute and conditional contraband they thought were lawful to seize if heading for their enemy

This simple division between objects of security concern became the basis for all control through WWI

– only in times of war

At end of WWII, it was the US military that began pushing for national and international export controls directed at the Soviet Union. This was seen as highly contentious internally, as the US had never had a peacetime control system in place, and was also resisted by some other Western countries, particularly in Europe, that relied more on mutual trade with the Soviets.

However, by 1950, the US had succeeded in establishing CoCom, the Coordinating Committee for Multilateral Export Controls, which was essentially NATO countries minus Iceland plus Japan, controlling the trade of militarily significant items with the Soviets and Chinese.

The control system was based on a set of lists of items, all of which were tangible goods, and if a company wanted to export controlled items to a controlled destination, it needed the permission of CoCom. The essential assumption was still that controls functioned as they did in the 16th Century.

CoCom existed from about 1950–1994, and was replaced by the Wassenaar Arrangement for Export Controls on Conventional Arms and Dual–Use Goods and Technology, based right here in Vienna.

It wasn't until the 1970s that states would start to think that export controls might be used on intangible items, like knowledge, particular knowledge and information related to controlled tangible items. We will get to that in a little while.

Ok, so much for a history of controls on goods and technology. How about secrecy?



Most societies that have developed a form of writing have also developed a form of secret writing, to convey meaning to some, but not all.

Most of the systems we know about are Western in origin, such as this skytale (sky-taly) used in ancient Greece [just wrapping a note around a pole of specific diameter]

or the substitution cipher used by Julius Caesar in ancient Rome.

But the use of secrecy to control scientific and technical development of security concern has an even foggier history.

The secret of Greek Fire was kept so well by the Byzantines that it is still lost today.

There is murky evidence that innovations in gunpowder and various weapons systems like cannon were kept secret in medieval Europe, at least when they were first developed.

State secrecy around the development of novel military items in the 19th and early 20th Centuries was commonplace, with the Manhattan Project to develop a nuclear weapon in the United States seen as perhaps the largest example. Another was the German enigma encoding machine: i.e. there was secrecy around how to produce a device that produced secrets.

But the state's interest in secrets around knowledge of things that were not specifically military items or related to the state (like diplomatic communications). . . that did not come along until the middle of the 20th Century, at least in the United States.

That was when secrecy of scientific and technical knowledge around perceived dual-use items became entangled in security governance systems.

Before jumping to that, however -> security and academic thought had already had a long history in the US and the world.



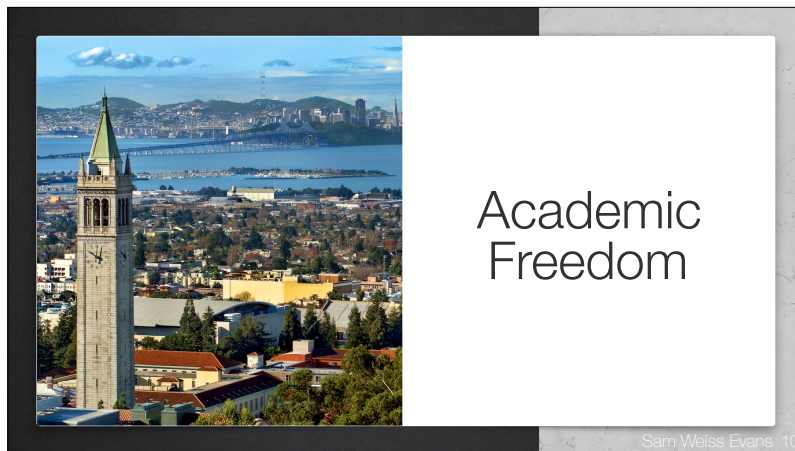
Scientists and scholars who push ideas that are seen as inimical to the ruling class have often been censored, such as Galileo's infamous trial in the 17th Century.

The first thing Hitler did in Poland was execute the intelligentsia.

In the US, it was McCarthyism of the late 1940s and 50s that sought to weed out Communist sympathizers from all areas of society, including academia, such as this meeting at the University of California to debate a loyalty oath all faculty had to sign, stating that they were not communist sympathizers.

There were also several US Congressional efforts to limit the engagement of foreign nationals in American research: Internal Security Act of 1950 (The McCarran Act) & Immigration and Naturalization Act of 1952 (McCarran-Walter Act)

But all of these efforts were pushing back at the idea, built up since the 19th Century, that academics have freedom to research, teach, and publish as they like.



Initial formulations of the concept of academic freedom can be found in 19th Century Germany, but it was the transportation, and subsequent modification, of these ideas in Post-Civil War American Universities, especially public and land grant universities, that formed it as the concept that has entered into the debate around security, science, and society.

In the US in late 19th and early 20th Centuries, American Universities banded together to produce a set of principles on academic freedom, and thus seed the idea that academia is a separate entity from society, where the right to research, teach, and publish shall not be infringed either by the state or even by the management of the university, that often being separate from the faculty in the American system.

Institutionalized by the American Association for University Professors in 1915, these arguments are often tied to both Enlightenment ideals of research, an in particular scientific research, as the search for truth, and the Mertonian ideals of science as Communal, Universal, Disinterested, and conducted through Organized Skepticism.

These views of what science is, how it works, and the relation of science to society have been a hotbed of research within Science and Technology Studies for over half a century.

One of my intents here, however, is to show how little that STS research has been incorporated into conversations around science and security. Much of the debate, even today, still rests on views of science and society that have their basis in the Enlightenment, Merton, and a 19th Century notion of academic freedom.

Attempts to govern science and technology of ambiguous security concern in the last 75 years

Sam Weiss Evans 11

By and large, the 1950s in the US was a time of optimism about the possibilities of science and technology. There was a belief that the large hosepipe of funding from the US government that turned universities into drivers of military innovation was transforming, thanks to the idea of the social construct for science and belief in the linear model of innovation, into a steady stream of funds for the production of knowledge and technology for society rather than just the military.

Efforts were made to declassify much research that had been advanced, and there was a general optimism in American society, whose infrastructure had been almost entirely untouched during the war, that anything was possible through science.

The late 1940s and early 1950s had another side, though, which saw the rise of anti-communist fervor, and a belief that the Soviets would stop at nothing to topple American democracy.

As I've already noted, the US was able to make the case to its Western allies that the transfer of military goods and the technologies needed to make them needed to be controlled to Communist countries. This control, however, covered only the tangible items themselves, from tanks to gyroscopes, but not the knowledge about how to make, use, or maintain them.

That didn't mean that there weren't also calls for controlling this knowledge of potential security concern.

The stage was set, in other words, for an argument between those who believed that the enemy was everywhere, and that everything was a potential threat, and those who thought that research which was free and open had nothing to do with the security of the state, or at least the scientists who conducted the research should not be told which ideas they could and could not pursue and share.

You can hear the the echos of the news articles I put up at the beginning.

While these conversations have been studied around primarily military science and technology, such as nuclear physics, I am looking at the edge cases, where there was a lot of contention about whether areas of science and technology should be considered security concerns, and whether that consideration should lead to stringent governance tactics.

The hunt to look for science that might have security implications, but was not itself related to militarily significant technology took several tacts in the first decade after WWII.

1950s Science and Secrecy

- Office of Strategic Information (1954-57)
- Atomic Energy Act of 1946, amended 1954
- Intelligence Community: *Committee on Exchanges (COMEX)*, mid-1950s

last January. When the plan for controls over the export of data was announced it was criticized widely as peacetime censorship. Officials of the strategic information office denied any intention to set up a censorship. Today's action exempts from validated export licensing requirements technical data dealing with dissemination of scientific information not directly and significantly related to design, production and utilization in industrial processes. Information so exempted, includes correspondence and attendance at meetings. Also exempted is instruction in academic institutions and academic laboratories.

Sam Weiss Evans 12

We could think of this as ACT ONE in the attempts to develop a governance mechanism around knowledge and information of indirect security concern.

OSI established 1954 in Commerce at behest of the National Security Council because of growing concerns about the Soviets obtaining information that was unclassified but still of strategic importance to the US in case another state got it and used it against the US.

At first, it saw its role as adding to the export control system a layer of control on information that may have a potential security significance, though not directly related to military technology. This control would be 'voluntary', and so not classified. OSI received immediate and wide negative cries from businesses, universities, and the press, all of which argued that what the office was doing was censorship and had no place in peacetime.

I want to take a moment to step back here, and work out why OSI didn't work. The US had just come off of years of near total government control of information flow, and there was a lot of resistance to reinstating that without clear democratic oversight. OSI's reports to the Secretary of Commerce, however, were themselves classified, even though they were supposed to only address unclassified information in their duties, and had no authority to be what are called 'original classifiers' themselves, i.e. they could not make information secret. These were also arguments made against OSI, as were later ones that claimed the head of the office presented himself in "a highly unrealistic attitude of cloak-and-dagger self-importance."

But these claims were also coupled to a belief that other forms of control, such as export controls and classification, were already adequate at addressing the perceived threats to national security of science and technology.

Not even three years later, its funding was pulled by Congress, after hearings where it was made clear even those working in the office didn't see its purpose anymore.

Nevertheless, the idea was there that there was a need for control on knowledge that might have potential for security concern, but did not directly relate to military technologies.

Other controls

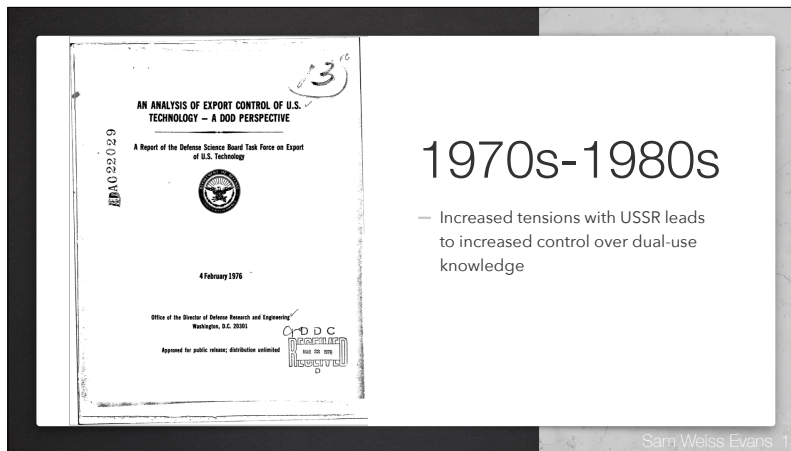
While the Atomic Energy Act was passed in 1946, it was amended in 1954 to include a "born secret" provision that covered "All data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy". While there was some pushback on incorporating nuclear energy controls as well, there was much greater awareness of the seriousness of atomic weapons, and that seems to have quelled the types of arguments about censorship that had prevailed over OSI.

Visas were, and have ever since, been one of the main mechanisms in practice on the international exchange of information. The Internal Security Act of 1950 (the so-called McCarran Act) and the Immigration and Naturalization Act of 1952 (the so-called McCarran-Walter Act) established rigid and indiscriminant restrictions on the issuance of visas to aliens seeking to enter the United States.

- These Acts were carried out in practice largely through the Intelligence Community's Committee on Exchanges, which was established at the same time.

So in this round, there were two groups within the government vying for control over who gets to determine the cases in the grey zone of whether science is a security concern.

- Commerce's efforts failed, due to a mixture of perceived incompetence and for being caught up in the debate on censorship. However, it was also at least a little more of a public entity than the intel community.
- Intel work happened largely behind the scenes, and seems to have been run such that it did not overly ruffle the feathers of academic freedom.



ACT TWO in the attempts to develop a governance mechanism around knowledge and information of indirect security concern happened nearly three decades later, and this time it was more directly related to export controls.

The 1960s and early 70s saw an increase in academic exchange and cooperation between the US and USSR, even in areas like nuclear fusion research.

This was part of the broader strategy of Detente

However, when the DoD saw these exchanges happening, they saw not an increase in security through the mutual sharing of knowledge, but the exact opposite!

They commissioned a report to understand how export controls might be used to limit this sharing of knowledge about how to make, not necessarily tanks and bombs, but the machine tools that could make them, and the computer manufacturing techniques and science of chip design that could result in expanded military capabilities.

Defense Science Board's Task Force on the Export of U.S. Technology's final report in 1976 (called the "Bucy Report" after its chair). The Task Force analyzed the risks to national security that might be posed by the expanded levels of trade witnessed in the early 1970s, and concluded that the control of the export of knowledge and information was as important as the control of the export of physical things, and thus the export control system, which to that date had only controlled the transfer of physical objects, could now be used as justification to control the sharing of scientific knowledge as well.

- assumed the point of controls was to maintain tech lead over the Soviets.

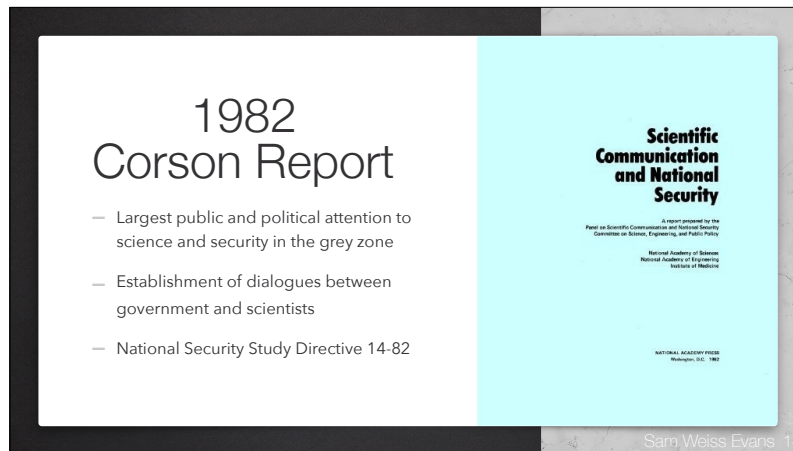
got enacted in Export Administration Act of 1979.

basic vs applied distinction in research blurring:

- microelectronics: fundamental physics research carried out side by side with novel processor development.
- Intelligence information that Soviets were trying to gain knowledge on knowledge of dual-use items.

This was all happening, however, in an atmosphere that was becoming increasingly hostile to military and intelligence funding of research.

- Vietnam, pentagon papers
- Universities were divesting from classified and military funded research



NAS Report on National Security and Scientific Communication

This report did more than anything prior to bring national public and political attention to intersection of science and security.

US economic and strategic competitiveness was strengthened, not diminished, but free exchange of ideas.

One of the big findings with Corson was that “a substantial portion of the problem between the government and scientific research community stemmed from a combination of ignorance of each other’s mindset and working environment and lack of channels through which to communicate.” (Wallerstein & McCray 1983? P. 22)

After Corson, several permanent and ad hoc mechanisms were established or modified to address this:

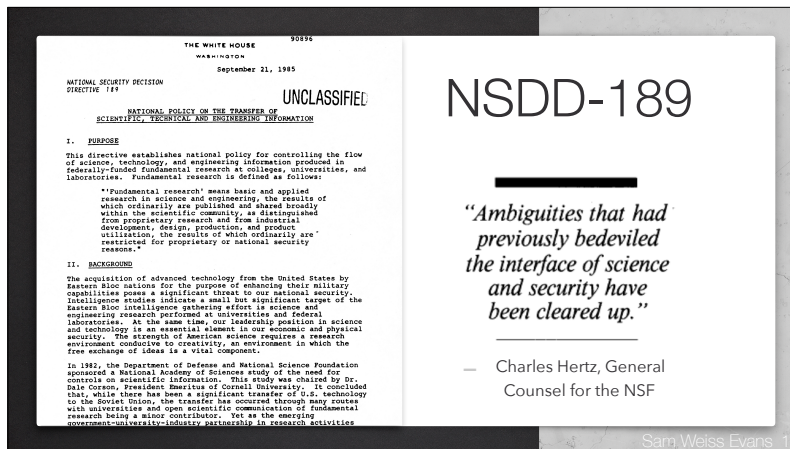
The Committee on Exchange (COMEX) Academic Advisory Group, which was an interagency committee run by the intelligence community to advise on whether visas should be issued to foreign scientists, did not itself have any scientists on in the Group! COMEX therefore established a panel of academics to consult with, [but it is unclear how regularly they have been consulted]

Dale Corson formed the Government–University–Industry Research Roundtable at the National Academy of Engineering to provide “a forum where scientists, engineers, administrators, and policymakers from government, universities, and industry can come together on an ongoing basis to explore ways to improve the productivity of the nation’s science and technology enterprise” <https://www.nae.edu/102578.aspx>

- still exists today <http://sites.nationalacademies.org/PGA/quirr/index.htm>
- Though it rarely touches on security issues now
- It is extremely high-level, not the people working on the ground

It also got the President’s attention, and Reagan established a committee (NSSD 14-82) in OSTP to figure out what to do. The committee’s work was classified, and it is unclear if they ever produced a report

- however in 1985...



Drew a clear line

Reinscribed the demarcation between scientific research and security

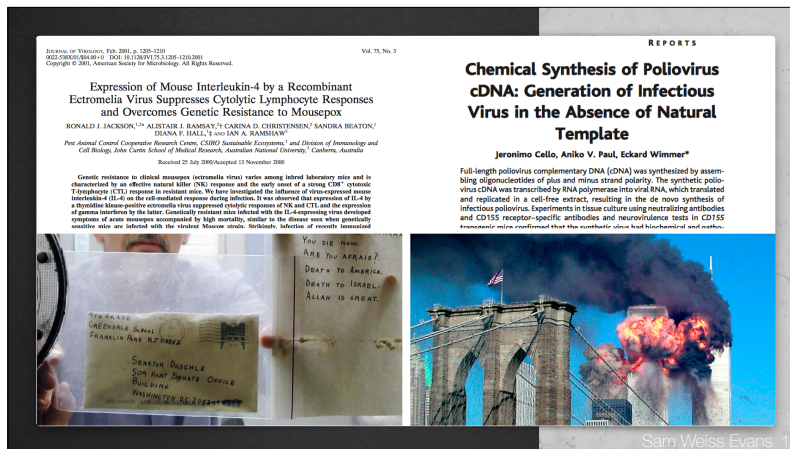
Became a referent point (boundary object) for the security and academic communities

It did not stop debate, but excluded fundamental research from discussion of security concerns.

Thus, It was nobody's concern if fundamental research presented security issues because, by definition, it did not.

It is worth pausing here to point out that most of the rest of the Western countries saw much of what the US was doing in this grey zone as far too complicated. The UK and Japan asserted that it was going well over the grey line in what knowledge it controlled. France and Germany thought the US was muddling a perfectly clear and simple divide. [Wallerstein et al 1987]

Then, in the early 2000s, several events occurred that would unsettle the line NSDD-189 had drawn in the sand.



We can think of this period as ACT THREE in trying to develop governance mechanisms around science of ambiguous security concern.

First, we have a new science being caught up in the debate: biology, and specifically genetic engineering.

biology drew a bright line around security concerns in the 1970s by the creation of the biological weapons convention, which outlawed the research and development of biological weapons. This was coupled with a recognition by scientists in the field that their work might cause harm unintentionally to themselves or their communities, and therefore they created a biosafety laboratory system and protocols. This focus on safety and lack of ability to overtly develop weapons led to an embedded myopia in biology towards even thinking about security issues in research. It also meant that unclassified biological research had largely flown under the radar of the security community.

2001

Early 2000s several papers and events catalyzed interest in security issues in biology

Synthesis of mousepox, poliovirus; Anthrax

These events raised awareness within the biological research community about what they called the “dual-use dilemma”, where all research could potentially be used for good or ill.

combined with 9/11 they created an impetus for massive government funding into biosecurity and biodefense research

National Science Advisory Board for Biosecurity (NSABB)

- Created in 2004 as a boundary organization between biology and the government on security issues
- Embroiled in 2011 H5N1 controversy
- Created concept of “Dual Use Research of Concern (DURC)”

Sam Weiss Evans 17

in NIH because of recommendation of Fink Report

The board advises on and recommends specific strategies for the efficient and effective oversight of federally conducted or supported potential dual-use biological research taking into consideration both national security concerns and the needs of the research community.

It was established as a scientific board with non-voting government members, including members from the intelligence community.

- government advisory body
- focused on security issues
- not in Commerce, Defense, or Intel, but NIH...
 - problem? NIH is main funder of research (\$40bil/year!)

Dual Use Research of Concern

A concept of lost opportunity



Sam Weiss Evans 18

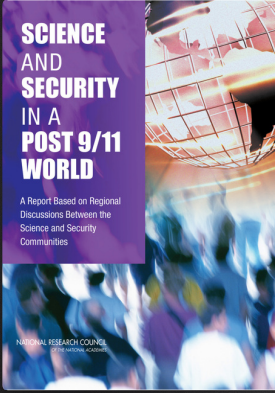
H5N1

“Life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security.”

in practice: 14 select agents and 7 experiments of concern

DURC could have gone the other way!

Since all research is DUR, let's focus on training and reshaping incentive systems



Taking Stock (and ignoring it)

- Recommendation 12: A deliberative, standing entity should be established to address ongoing shared concerns of the security and academic research communities...

Sam Weiss Evans 19

Let's take stock here:

It's 2007.

- The guiding image of both science and politics in the US now is one of a globalized world
- a growing belief that the US was not the world leader it once was
- the cracks are starting to show on state-based approaches to security around scientific work
- growing attention is placed not on the latest and greatest, but also on how the mundane can be turned into security concerns, like planes, fertilizer, and box cutters.
- visa and export controls are no longer seen adequate to stop all potential security concerns in science mainly because by the time we figure out it might be a concern, the knowledge has already disseminated beyond the state borders.
- The new NSABB is working on how to govern in this space, but just in biology

This NAS report pointed out that what we really need is a cross-the-board and internationally-facing Science and Security Commission.

this entity was never created.

Current efforts to rethink the governance of security concerns in science & technology

Sam Weiss Evans 20

shift to what we are doing today

this is a personal journey

because I'm wondering how to build a security governance system in the grey zone

and I think that by being involved in it I can both bring STS expertise, and greatly refine STS concepts through practical feedback loops

Look at the work of two orgs: FBI and iGEM



FBI

Safeguarding science

- need to talk to sci
- don't be the people breaking down doors
- but the people you turn to to help ensure you're not causing harm
- global
- public

- but unresearched.



- Security comes from understanding the sociotechnical networks your research exists within
- Building broader awareness from day one
→ shifting global training in bioengineering
- Sandbox for global experiments on governing security concerns



Sam Weiss Evans 22

basics of igem
student competition
6000 students a year
40 countries
over 10 years

HP filled with scientists, policy experts, ethicists, social scientists, people with little experience of iGEM
— iterative learning and experimenting process over years

this iteration needs to be more public.

Questions?

Sam Weiss Evans

- Assistant Research Professor
STS Program, Tufts University
- Research Fellow
STS Program, Harvard University
- sam@evansresearch.org

