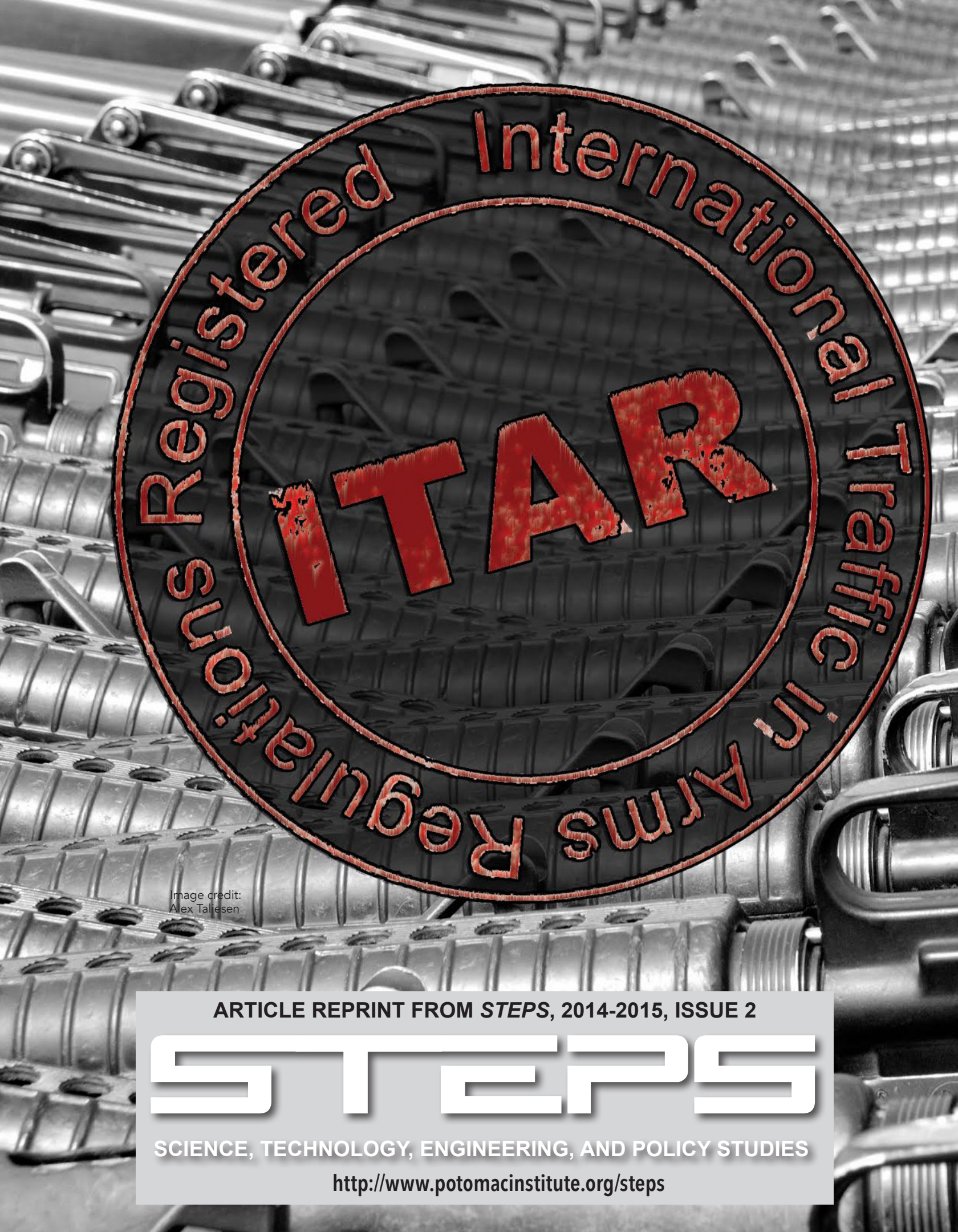

Image credit:
Alex Taliesen

ARTICLE REPRINT FROM *STEPS*, 2014-2015, ISSUE 2

STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

http://www.potomacinstitute.org/steps

The Decline and Fall of the ITAR Empire

The authors take on ITAR, the International Traffic in Arms Regulations. ITAR places burdens on researchers, to avoid export of information about a large range of technical topics that can relate to military systems. Since an export can amount to nothing more than showing a viewgraph at a domestic conference, or sending an email to a colleague, ITAR casts a dark shadow over US research. While reform efforts are moving slowly, this article dares to make an obvious conclusion: That ITAR must be completely rescinded. The case is made that ITAR, by virtue of restricting information, is more harmful than good, and that other mechanisms and laws exist to protect secrets and systems for national security purposes.

Robert Hummel, PhD, Richard Pera, and Charles Mueller, PhD

INTRODUCTION

The International Traffic in Arms Regulations (ITAR) is collapsing from excessive bureaucracy. Beginning in 1976 as a heavy-handed attempt to restrict both transfer of physical munitions and disclosure of information about munitions, the subsequent introduction of thousands of amendments turned ITAR into a monstrosity of complexity that typifies regulation gone amuck. Not only is it collapsing because it is unwieldy, it is also outmoded in its attempts to restrict the flow of information.

The original purpose of the export control system, of which ITAR is a major component, is to "promote our national security interests and foreign policy objectives."[1] As a result of the system, anyone wishing to export any product, item, idea, or to disclose information, to any foreign person whether in the US or abroad, must be concerned with the potential need for an export license, or whether the item is subject to export control.

The main lists that describe "articles" to be restricted are the United States Munitions List (USML) and the

Commerce Control List (CCL). ITAR deals with the USML. Administered by the State Department, the Department of Defense is particularly concerned with the USML, through the Defense Technology Security Administration (DSTA).[2] A history of ITAR's evolution and convoluted association with multiple federal agencies can be found in an MIT open access paper.[3]

There are complex regulatory processes whereby restrictions are updated and lists are examined and modified. Congress regularly passes laws calling for updates to the regulations, which are then assembled in amendments. In 2010, an interagency review determined that the overall export control system in the US is, to put it politely, a mess.[4] Reportedly, the review said that the current system is "overly complicated," redundant, and "in trying to protect too much, diminishes our ability to focus our efforts on the most critical national security priorities."[5] Secretary Robert Gates said that the system is a "byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government."[6] Accordingly, the President's administration announced an Export Control Reform Initiative in 2011.[7] The result has been a flurry of Federal Register notices and ongoing reviews of each of the 21 categories of the USML.[8] Reform of each category is subject to public comment, and categories and other reforms are being addressed incrementally, as documented by the government's export.gov website.[9]

Reforms are being pursued slowly and methodically, with incremental updates to the current structure of the ITAR Empire. Commenting on the initiative, the US Chamber of Commerce observes that the "the US export controls regime has long covered too many products that lack a significant military application or are readily available from other countries. The United States should eliminate controls that serve no real security purpose."[10] That does not seem to be happening. Instead, some categories are being updated, and lists are being consolidated and made easier to access. However, information in 21 categories will still be restricted.[11] The well-meaning reform initiative, which has plodded along for six years at this point, has devolved into tweaking of vague descriptions of poorly understood technologies that support a grotesque framework of patched-together regulations and misguided directives.

This framework is based on many complex definitions, bureaucratic insertions, and amendments. For example, ITAR makes a distinction between a "US person" and a "non-US person." A "US person" involves a convoluted definition that includes US citizens, many people with "US permanent residency," and certain corporations that are predominantly located in the US (Yes, a US person is not necessarily a person.) There are further complications involving "dual nationals" and "third country nationals," for so-called "third party transfers."[12] The law makes a distinction among different classes of weapons, including "Significant Military Equipment" (SME), and the Missile Technology Control Regime Annex (MTCR),[13] along with the Department of Defense Military Critical Technologies List (MCTL) and the Developing Science and Technologies List (DSTL).[14] The 21st category in the USML is titled "Miscellaneous Articles," which includes "any article not specifically enumerated in the other categories" with military applicability designed for military purposes, or technical data or services related to such an article.[15] Finally, there are different categories of foreign people, which need to be accounted in terms of a potential transfer. For example, a university can disclose ITAR technical data to a foreign person who is a full-time employee (e.g., postdocs), providing certain procedures are followed and that the employee is not from a country to which the United States observes an arms embargo, which includes China.[16] A similar complication arises with respect to dual nationals who are employees of an

"The fact that economic interests might be in conflict with national security concerns is a seed of anxiety."

end-use company that has been approved for an export of a product or technical data.

It is easy to complain about the many bureaucratic layers that are embedded in ITAR. The complexity is such that observance of ITAR is rarely based on observation of its provisions, but rather out of fear of prosecution from inadvertent transfers. Further, its outdated provisions undermine its credibility as an effective tool for export control. The reform initiative will not change that reality.

DEFENSE ARTICLES AND INFORMATION

Our main interest in this article is with the restrictions that ITAR imposes on the transfer of information. The convergence of systems and information is such that ITAR's primary effect is to restrict the free flow of information; the export of actual defense systems is typically regulated by treaties, agreements, and other export control provisions.

ITAR prohibits the export of defense articles and defense services, as carefully defined in Part 120. Defense articles include technical data concerning items on the USML. Technical data includes "information…required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation."[17]

Technical data is thus explicitly information. This can manifest in viewgraphs, verbal presentations, or digital data on an accessible server or in an email message. Note that the original definition predates the Internet age, before information is easily sent across borders and among colleagues digitally. Whereas the regulations envisioned the transport of hard documents and physical presentation of information, now an email can be considered a defense article.

ITAR explicitly does not apply to basic knowledge taught in schools. As written in the regulations, however, this exception would not apply to research that discovers new knowledge. Thus ITAR inhibits research at universities that might otherwise apply to defense systems, when foreign graduate students might be involved.

ITAR further restricts defense services, which include "the furnishing to foreign person of any technical data controlled under this subchapter…whether in the United States or abroad."[18]

Accordingly, an email sent to a colleague across the hall, who happens to be a foreign person, can be a prohibited defense service. Release of technology within the borders of the US is called a "domestic export," or, as defined by the Department of Commerce, a "deemed export."[19] In its current incarnation, a violation of ITAR need not be an intentional service to a foreign entity, but rather a simple and potentially unwitting transfer of information.[20] Further, once an article (whether a system or information) is subject to ITAR, it is restricted from further export no matter where it is – re-export requires a license.[21] ITAR has global reach.

ITAR TECHNICAL INFORMATION

The genesis of ITAR, and of the related Export Administration Regulations (EAR), go back to the Arms Export Control Act (AECA) of 1976,[22] which builds upon a series of Export Control Acts dating back to 1940.[23] The 1976 act gives the executive branch the authority to control exports of "defense articles and services." This responsibility was subsequently assigned to the Department of State. The intent of the legislation, developed amidst the Cold War, was to restrict sales and "trafficking" in military equipment and services so as to lessen the likelihood of regional conflicts. It was designed to help promote US economic interests, which include assurance of military equipment sales to friendly nations. The fact that economic interests might be in conflict with national security concerns is a seed of anxiety.

The AECA actually seeks to promote cooperation among friendly nations for mutual defense, including sharing of defense information and research results.[24] While the original legislation does not provide definitions for "defense articles" and "defense services," enabling regulations and subsequent amendments make clear that definitions can be found in Section 644(d) and (f) of the Foreign Assistance Act of 1961 (22 U.S.C. 2403). Defense services include information that is transmitted for the deliberate purpose of providing military assistance. Information, according to the act, is defined as follows.

The U.S. Code states: "'Defense information' includes any document, writing, sketch, photograph, plan, model, specification, design, prototype, or other recorded or oral information relating to any defense article or defense service, but shall not include Restricted Data as defined by the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 et seq.], and data removed from the Restricted Data category under section 142d of that Act [42 U.S.C. 2162(d)]."[25]

Thus, when we speak of ITAR technical information, we mean "defense information" that relates to an article restricted by ITAR (i.e., related to an article on the USML). ITAR prohibits providing technical information to a foreign national, whether in the US or abroad, based on an assumption that the information will knowingly provide military assistance.

The news media and those subject to its restrictions often ridicule the fact that defense articles include technical information, such as the inclusion of software and encryption technology on the USML.[26] Non-military systems that contain USML components themselves become ITAR restricted, which induces foreign manufacturers to use non-US components in order to advertise their systems as "ITAR-free."[27] This encourages US companies to avoid participating in defense work for fear of tainting their products with the ITAR label.[28]

Systems and information are increasingly equivalent, as information to make a munition becomes tantamount to the ability to acquire that weapon. Since nearly any system can be reverse-engineered given sufficient diligence, possessing a weapon system amounts to having the information about that system. Thus ITAR became strongly restrictive of the export of technical information. Effectively, the migration from controlling the export of physical articles to controlling the disclosure of information was necessary, as information became the dominant source for acquiring systems.

There remains an underlying assumption in ITAR concerning information about USML articles, that the US maintains technical dominance in each area. It makes no sense to protect information when adversaries have superior products and thus superior information. Historically, the United States excelled in areas of technology, such that the USML exclusively contained articles for which the United States was the world's leader. Although the USML is updated from time to time (and is so mandated in the original legislation), it is not maintained with sufficient technical understanding of the international landscape. Indeed, ITAR is a powerful incentive to foreign friends and adversaries alike to develop their own military technology research programs. Further, certain communities have complained that by restricting their sales market, ITAR has impeded their technological development for subsequent generations. Examples include the fields of satellites[29,30] and high energy lasers,[31] potentially causing the United States to fall behind competitors.

Nevertheless, we maintain that there is often a need to restrict the transfer of information. It is one thing to sell a missile to an adversary such that it might be used in a conflict against us, but it is quite another to provide the information needed to manufacture, sell, and utilize thousands of missiles. Since digital information is so easily shared, and with the coming possibility of providing files of data that permit the near-instant manufacture, via 3-D printing, of true defense articles, it becomes more urgent than ever to ensure that information pertaining to munitions, weapons, and national security be kept truly secure. The current lists (the USML and CCL) do not, however, appropriately differentiate between what needs to be protected, and what can be safely made open source.

There are proposed changes to the definitions of ITAR "technical data" that would strengthen legal sanctions against sharing design files, such as 3-D printable guns.[32] These changes would attempt to systematize the differentiation between information that should be kept secure versus what can be posted. However, because the onus of interpretation is left to the person possessing the information, enforcement is likely to be capricious and post-facto.

As a result, our current treatment of technical information is haphazard and irrational. We attempt to protect "Sensitive But Unclassified" design data for the F-35, only to discover that Chinese cyber warriors pillage the networks for intelligence to speedily develop their own jet fighter.[33] We actively collaborate with the Chinese on advanced thorium-based molten-salt cooled nuclear power plant development, which will help modernize its navy.[34] We decry Chinese censorship

of the Internet, and yet we expect US researchers to self-censor their postings of research results.[35]

At issue is whether ITAR is the appropriate discriminant of information that should be secured. If so, at what cost?

THE BURDENS OF SECURING ITAR TECHNICAL INFORMATION

ITAR places the burden on the developer, researcher, or person possessing information. Essentially, every US person is expected to know and understand the USML in order to prevent transfer of ITAR technical information to a non-US person. Since an export occurs with a mere email message or verbal communication, ITAR expects total familiarity with the USML, and for researchers in certain fields to exercise great restraint in scholarly communications.[36]

There are recurring concerns over the constitutionality of the implied prior restraint on free speech imposed by ITAR.[37] These concerns have only been heightened by recent reform efforts.[38] While the First Amendment does not protect speech that divulges classified information, as early as 1981, the Department of Justice warned that technical data disseminated by someone "unconnected with any foreign enterprise" to a foreign person, even when it is known that the information may be used in the manufacture or use of arms, is protected free speech.[39] Because ITAR is enforced through prosecutions[40] and threat of prosecutions, it denies rights guaranteed by the Constitution when it inhibits speech that poses no grave and immediate threat to national security.

Further, every industry, small business, and university lab that engages in defense research work, together with all people in those organizations, must track the "US-person" status of every staff member and every visitor.[41] Conferences and presentations concerning defense research will often need to restrict attendance, and must again be cognizant of the status of each attendee. Universities with foreign graduate students and postdocs, many of whom are awaiting green cards, must carefully consider whether they will accept contracts and grants that sponsor research related to defense technologies, for fear of inadvertent violations based on domestic export of unclassified information.

This might not be such a burden if the USML were clear and concise, and if the distinction between defense work and commercial research were well-articulated. But the increasing globalization and convergence of technology research with multi-use objectives makes discernment with the USML impossible. The lack of US-personhood identity cards means that the regulations are dependent on foreign persons declaring that they are foreign. As a result, compliance is based on guesswork. And if the US lead in technical areas of the USML were still as commanding as it once was, then protecting the information from disclosure would still make sense. But we are now largely protecting outdated information.

The costs of ITAR are not just the encumbrances of compliance, nor the opportunity costs of the work that might be done in place of compliance efforts, but also the missed opportunities caused by behaviors undertaken to avoid being covered by the law.

Both domestic and foreign industries avoid purchasing American components in order to develop versions of their products that are "ITAR-free."[42] US multinationals have been establishing research centers abroad, in part to enable research by non-US persons in directions that might be subject to ITAR if performed domestically by US employees.[43] ITAR not only suppresses commerce by restricting foreign sales, bust also erodes America's technological dominance by inhibiting our best scientists and researchers from collaborating on a myriad of technical areas.

The costs of ITAR information restrictions would be justified if it truly protected information that needs to be kept secret. The Department of State views the restrictions as a "classified lite" system, with less onerous control mechanisms compared to the security apparatus that implements our classification system. The security laws, however, are very clear: if the material is classified, it must be handled in specific ways. There is a high degree of confidence (and empirical evidence) that it will not be transferred to those ineligible to receive it. Only those dealing with classified information must be concerned with the rules for handling classified information, and the decision as to what is classified is up to original classification authorities. ITAR information, on the other hand, is of concern to everyone who

comes into contact with information that might relate to any of a long list of systems and technologies with military applicability. The burden of dealing with ITAR may be only one-fourth of the burden of dealing with, say, information classified at the confidential level per person. But the burden may fall on a hundred times as many people, and thus cost society many times more than simply classifying the information.

A WAY FORWARD

Reform of ITAR and the export control system is laudable, but happening at a pace that is slower than the pace of technology. The reform initiative has already failed.

ITAR is outdated. By trying to control information dissemination in addition to the export of physical systems, it has failed to adapt to an environment where technology changes rapidly, is nearly always of multiple use, and has near-instantaneous reach anywhere on Earth.

To control the export of physical systems, the legislation, treaties, and authorities that fund the development of the systems (i.e., the Department of Defense) can readily ensure that weapons do not fall into the wrong hands.

In order to control information flow, there is an existing system. The existing system actually works, as opposed to a poorly contrived ITAR system that attempts to limit the flow but in fact may facilitate theft or adversarial development of information. The system that works is based on the security law of 1947 and its implementing regulations.[44] When information is classified, it is generally kept within channels for a long time, and works to protect the information. ITAR restrictions, on the other hand, most likely offer no protection at all.

Indeed, when we secure ITAR information on unclassified systems that are bundled and marked as ITAR, there is a sense in which we have enticed others by affixing a "steal me here" label.

Security laws include a level of classification called "Confidential," which is defined as material that would damage national security if disclosed. These laws also acknowledge other forms of restrictions, such as "Controlled Unclassified Information," "Restricted," and "For Official Use Only." Major defense acquisition projects have "program protection plans" that include protocols to protect design information. It would seem that security laws have sufficient mechanisms to protect information, if only that information were assessed and labeled at its creation. ITAR provides an excuse to forego appropriate classification of technical information, which results in the lack of protection to a substantial amount of data that should be protected using the classification system.

If we classify technical data that is currently labeled as ITAR, then only those with appropriate security clearances will be able to access and work on the technology. Right now, a US security clearance is only available to US citizens, and not US persons. (However, the background check required for a position of "Public Trust" might suffice for non-citizens.) Further, material can only be classified if its disclosure will cause harm to US national security. Whether these are the appropriate criteria to ensure security is a matter for the security apparatus. Central to this argument is that there already exist constitutional and effective means of protecting information without a burdensome and cumbersome ITAR.

Of course, the best defense is one where we possess the best weapons and best technology, and maintain dominance by adapting, updating, developing, adopting, and integrating new technologies faster and more efficiently than any other nation. Rather than facilitating our dominance, ITAR has become a burden to our advancement.

We should classify at appropriate levels that information that should be protected, and permit open and widespread collaboration on topics where it benefits us to stay current.

CONCLUSION

The conclusion is that ITAR must be completely rescinded. Reforming ITAR will not fix its flaws. Its categories and lists cannot be kept current at the rate required to be rational. By confounding systems and information, ITAR has become an impediment to the development of technology, thereby threatening to upend US dominance in technical areas that are relevant to national security. By attempting to protect information from communication – even in lectures and email correspondence – ITAR has allowed information that should be classified to remain unclassified. Furthermore, through intimidation it restrains legitimate research and collaboration, including among US persons, which are vital to our economic and security future.

To truly control the trafficking in arms, we need to pass and enforce laws that control foreign arms sales, based on specific systems. When component technology needs to be protected, the information required to make that component should be classified. Thus export of systems with sensitive component technology should be controlled by means of security laws. When information needs to be protected from disclosure because it could harm our national security, that information should be classified at the appropriate level.

These are common-sense steps that would greatly benefit our national security and economic prosperity. The decline and fall of the ITAR Empire is well underway and inevitable; let us not allow its obsolescence to crumble our country, too.

NOTES

1. US Department of State, "Overview of U.S. Export Control System."
2. Office of the Secretary of Defense, "DTSA Mission."
3. Morgan Dwyer, Gwen Gettliffe, Whitney Lohmeyer, Annie Marinan, Erik Stockham, Annalisa Weigel, and Kerri Cahoy, "The Global Impact of ITAR on the For-Profit and Non-Profit Space Communities." International Astronautical Federation, 2012.
4. Export.gov, "About Export Control Reform."
5. Leigh T. Hansson, ESQ. and Michael J. Lowell, ESQ., "Top Ten Things to Know About Export Control Reform," Association of Corporate Counsel, June 01, 2011.
6. "Robert M. Gates' Speech Before the Business Executives for National Security, April 20, 2010."
7. Export.gov, "About Export Control Reform."
8. US Department of State "Export Control Reform."
9. Export.gov, "Export Control Reform News."
10. US Chamber of Commerce, "Modernize Export Controls," last modified May 19, 2015.
11. The unofficial updated USML is maintained at "Electronic Code of Federal Regulations." The unofficial CCL is maintained by the Bureau of Industry and Security, US Department of Commerce at "Export Administration Regulation Downloadable Files." The official list is the annual baseline publication together with all amendments in the Federal Register.
12. US Department of State,"Third Party Transfer Process and Documentation."
13. See Part 121.1(b) and (c): "The International Traffic in Arms Regulations (ITAR)."
14. "Funding Cut, Military's List of Critical Defense Technologies Languishes," *The Security Ledger*, January 25, 2013.
15. Part 121.1, Category XXI, "Miscellaneous Articles."
16. 22 CFR Part 125.4 (10), referencing 22 CFR Part 126.1, (a): "The International Traffic in Arms Regulations (ITAR) Part 125."
17. "(ITAR) Part 120.10."
18. "*Ibid*, Part 120.9."
19. Refer to §734.2(2)(ii): "Export Administration Regulation §734"
20. Zlatko Hadzismajlovic, "Foreign Nationals and Defense Hiring: The Most Delicate of Decisions," *New York Law Journal*, August 6, 2012.
21. Bureau of Industry and Security, US Dept of Commerce, "Guidance on Reexports."
22. US Department of State, "The Arms Export Control Act"
23. "This Day in History: July 5th, 1940: United States passes Export Control Act." History, A&E Networks.
24. See 22 U.S.C. § 2751 "…facilitate the common defense by entering into international arrangements with friendly countries which further the objective of applying agreed resources of each country o programs and projects of cooperative exchange of data, research, development, production, procurement, and logistics support to achieve specific national defense requirements and objectives of mutual concern."
25. 22 U.S.C. § 2403(e)
26. Dan Froomkin and Amy Branson, "Deciphering Encryption." *Washington Post*, May 8, 1998.
27. Steven Brotherton and Karen Server, "Beyond reach? How to develop ITAR-free systems." *World ECR* 1 (2011): 16-19.
28. "ITAR Amendments Undermine Key DOD Acquisition Goal." *Defense Trade Law Blog*, March 18, 2015.
29. Ryan J. Zelnio, "Determining the Effects of ITAR Regulation on Commercial Space Manufacturing." Paper presented at the Interdisciplinary Graduate Student Conference: Science and Technology in Society March 31-April 1, 2007.
30. Richard Kusiolek, "ITAR Dilemma: Finding The Balance Between Regulation And Profit." *Via Satellite*, July 1, 2008.
31. Martin Seifert and Anthony Rallo, "Market Insights: U.S. military high-energy laser development hindered by ITAR regulations." *Laser Focus World*, June 1, 2015.
32. Brian Krassenstein, "US Government Proposes ITAR Amendments to Choke Off Distribution of 3D Printable Gun Models." *3DPrint.com*, June 8, 2015.
33. David Alexander, "Theft of F-35 design data is helping U.S. adversaries-Pentagon." *Reuters*, June 19, 2013.
34. Mark Halper, "The U.S. is helping China build a novel, superior nuclear reactor." *Fortune*, February 2, 2015.
35. Sharon Weinberger, "Export-control laws worry academics," *Nature* 461 (2009): 156.
36. Beginning in the 1990s, this was a major concern for number theorists working on encryption algorithms. A court case based on infringement of first amendment free speech resulted in changes to the export administration regulations; See Daniel J. Bernstein v. U.S. Department of Commerce, et al. Second Supplemental Complaint.
37. "ITAR Control of Public Speech." *Defense Trade Law Blog*, June 3, 2015.
38. Andy Greenberg, "3-D Printed Gun Starts The War Between Arms Control and Free Speech," *Wired*, May 6, 2015.
39. Constitutionality of Proposed Revisions of the Export Administration Regulations.
40. Thaddeus McBride and Reid Whitten, "Prison Time and Export Control: University Professor's Case Illustrates Dangers of Ignoring Export Compliance." *Government Contracts, Investigations & International Trade Blog*, Shepard Mullin, October 24, 2011.
41. See section on "Criticism of the Current Rule" in John M. Hynes, "New ITAR Rule on Transfer of Defense Articles to Dual and Third-Country Nationals Creates Substantial New Compliance Obligations," *Government Contracts, Investigations & International Trade Blog*, Shepard Mullin, June 16, 2011.
42. Richard Kusiolek, "ITAR Dilemma: Finding The Balance Between Regulation And Profit." *Via Satellite*, July 1, 2008.
43. See section on "The Growth of Foreign Research Centers of U.S. Multinationals" in Wessner, Charles W. and Alan Wm. Wolff, eds., *Rising to the Challenge: U.S. Innovation Policy for the Global Economy.* (Washington, D.C.: The National Academies Press, 2012).
44. Stephen A. Cambone, "The National Security Act of 1947– 26 July 1947." A New Structure for National Security Policy Planning. Washington, D.C.: CSIS, 1998. 228-32.