David Aitel, Immunity, Inc. -- Comments for ETRAC meeting October 15, 2015:

First, I want to add some context to this reply: I am the CEO and Founder of Immunity, which sells Penetration Testing products and conducts commercial Penetration Testing and security assessments, and has for 12 years. Previously, I was a Computer Scientist at the National Security Agency, which provides me with a unique view on how both the Government and Commercial sector works with regard to these specific kinds of software tools.

Questions to be addressed:

1) Is it possible to interpret proposed ECCN 4E001.c. and the definition of "intrusion software" in such a way that legitimate cybersecurity research would not be affected?

As worded, our analysis is that legitimate cybersecurity research would be greatly affected. In addition, the kinds of tools we sell and use are used operationally, to help secure firms both large and small. They are required by PCI and other global security standards. All of these things would be massively impacted - and we think our reading is both accurate and comprehensive into the proposed wording and interpretation of the regulation.

2) Is it possible to develop a license exception, including but not limited to deemed exports and intra-corporate transfers, that will allow legitimate cybersecurity research to proceed without licensing delays and compliance burden? If so, what are the provisions of such a license exception?

The main issue, in our opinion, is that a large part of the regulation's wording aims to technically differentiate between "good" and "bad" intent for software tools. But Penetration Testing tools are by design as closely built as possible to intrusion tools. What differentiates them is not some magical feature set but who uses them, and against whom. Penetration testing tools have a command and control, a trojan or several trojans which each try to prevent themselves from being detected, and the ability to control remote machines - often, but not always including exploits, including "0day", the ability to pull information from those machines, and the ability to modify information on those machines and attack other parts of the network. These are the features the market-place demands to provide them with the most accurate and comprehensive tests, which they use to help secure themselves.

For example, a penetration testing tool must be "specifically designed" to bypass network monitoring (one of the ones we make has five different ways to do this built in). "Extraction of data" is such a broad term that all software tools in this space must do this. Dr Bratus is correct (in my opinion) in that a tool that does not attempt to bypass network monitoring cannot provide a relevant test for the customer! In fact, our customers often use anti-virus reports on how

nation-grade intrusion software works as requested feature lists for our product line. Google gets hit by the Chinese intruders daily, and they need a controlled tool that can help them model that threat as closely as possible. And of course, it's not just Google. It's every company in America.

The proposed interpretation white-lists "jailbreaking" as a legitimate use - and it MUST do so because jailbreaking cannot be done any other way than by using intrusion tools. But it is just one, minor, legitimate use of this kind of technology. There are many, many more that are done today, and there may be even more in the future. Five years ago nobody would have considered how important it was to have the ability to use intrusion tools to jailbreak your own phone. But the same technology may be required to tune your car in the near future.

Where these tools differ from the intended restricted set of tools is that they are used on computers that you are legally allowed to test. In other words, the difference is "intent", not some technical set of features. So when people try to make a license exception that would not drastically hurt standard operational practice, they try to make a carve out for the intent of the user. "Jailbreak" is in fact more a matter of "intent" than any specific technical carve-out - as evidenced by how many penetration testing products simply re-use the exact exploits provided by Chinese jailbreak teams.

Keep in mind, this is a rapidly changing field, and what may seem "highly advanced and sophisticated" today, is really just a line item feature in common toolsets tomorrow.

Likewise, all of these tools are built internationally, and used internationally. When testing a large financial, if you secure only the US portion of the network, you have accomplished nothing. The risk is spread out across the entire corporation, much of which is stationed overseas. This is one of the reasons export control is such a poor tool for examining this kind of software and process.

3) Is there a license requirement (combination of destination/end user/end use) and regulatory interpretation that would address the exchanges of technology that are of concern (i.e., those not intended to ultimately improve cybersecurity) that would result in no licensing burden on legitimate technology exchanges?

I don't believe a simple interpretation change would make any difference. In particular I am worried about any kind of special purposing of the idea that "public" exchanges of information are good and "private" is bad. Almost all commercial penetration testing and security consulting work would fall under "private" exchanges of information, and most of this is done in an international setting! Likewise, almost all security work is done as a collaborative effort among many teams, and trying to interpret "public" versus "non-public" work is quickly impossible when combined with the legal requirements of NDA's and other commercial agreements.

In addition, there is no “one vendor” or “one public”. Trying to interpret these words in a legal and regulatory context seems prohibitively complex.

Technology exchanges done in the commercial consulting world are not only “legitimate” but also a **fundamental security practice**, required by regulations but also by common sense Best Practices for every organization seeking to protect their networks and information.

This kind of software is often used in security trainings as well. You sit a whole class of people down with a fake network and ask them to hack it and look at the defenses and how they operate. Students are often international - and these classes are even sometimes conducted over WebEx sessions. In fact there are hugely popular international competitions for “Capture the Flag” efforts that include software that would be captured under the current proposed wording of the regulation.

The end use that you want to restrict is that of “software that is used against unwitting innocents, against their permission”. If you add “Software that is used for security research, penetration testing, or otherwise with the implied or expressed legal permission of the parties involved is exempted” to every location needed within the regulation, you protect current industry practice, but there are also many other complementary issues with any attempt of this nature. We would caution against trying to whitelist a long set of “legitimate practices” because this will no doubt miss important examples as well as be rather ambiguous in the end. Is the very useful tool SQLMap a “Fuzzer” or “intrusion tool”? Reasonable experts could disagree.

4) If none of the measures above would be adequate, what changes to the control text, including the definition of "intrusion software," would be required to ensure that legitimate cybersecurity research will not be affected?

Defining the “intent” of software is a notoriously impossible thing to do. It **violates some basic tenets of computer science** (for which Turing is most famous for). This is one reason two experts can debate the meanings of the definitions of many of the technical terms in this space and both be reasonably correct. I worry that what happened to the professor at Temple could very easily happen to anyone in our space doing the normal course of their business, as a result of the proposed regulation.

What is more likely to be successful is to regulate (via export control or another, more apt method) the operational use of tools to address human rights issues. I have spent the past 15 years building both kinds of tools - and the difference is not what the tool does, but who uses it, and who they use it against. One major operational practice is, of course, finding an attacker’s tool in use and sending it around the world to everyone to help analyze it! This is impossible to control with any regulatory language that does not take the intent of the user in mind. It reminds me a bit of the common April 1st geeky joke about a new proposal to include an “Evil Bit” on all packets that include an exploit, so they can be dropped by firewalls.

The joke is funny because it attempts to define the undefinable, which is humorous in a technical context. But in this proposed regulation's case, it is not a joke, and not funny. Instead it threatens the entire security industry and is particularly hard on the penetration testing community. While various proponents of the regulation feel that our concern is because we do not properly understand the regulation and proposed interpretation of the regulation, we feel they are mistaken. Not only have we hired expensive lawyers to examine the proposed wording, we have read it carefully ourselves, and compared it to both current-day and future possibilities.

Keep in mind, intrusion software sold for criminal purposes already puts the developer at risk under the RICO statutes, and this has been successfully prosecuted in the United States many times. The case of Stephen Watt with regards to the "TJMaxx" hacks is one notable example and was highly publicized. Of course, sales of any kind to Sudan are already restricted as well.

In conclusion - I apologize for how long this reply is, but many of these issues strike to the heart of the kinds of work and research we have been deeply involved in at Immunity. We are always available to discuss any more detailed technical examples at either dave.aitel@gmail.com, dave@immunityinc.com, or +1-786-263-9749.