Ladies and Gentlemen, esteemed Members of the European Parliament and of the European Commission.

It is an honor for me to be here and have the opportunity to speak before you on this very important topic. For the past 10 years I have worked in the Information Security industry as a Security Researcher and what follows in this talk derives from my experience in the field.

It is not customary for me to do scripted talks, but I believe the argument is of high enough importance to deserve a written exposition – you will forgive me for reading my notes.

I would like to begin my short briefing with a few premises on the topic of intrusion software and its regulation. I will then put forward a number of suggestions that my colleagues Thomas Dullien, Georg Wicherski, Stefano Zanero and myself have developed in the past few months.

As most of you here, I strongly believe that software, as most things in science and technology, can be employed for ill-intentioned purposes and I strongly believe that the EU and the Rest of the World should regulate improper use of code especially in relation to human-rights violations.

On the other hand, I am part of the school of thought that believes that code is speech and that speech should be free. Most, if not all, intrusion software is code and hence I posit that it largely should be free. Therefore I argue that the debate over software regulation is not particularly dissimilar from the debate on regulation of hate speech and as such it poses numerous important challenges.

I would also like to add, for the record, that export controls have proven to be highly ineffective and counter-productive for cryptographic software in the past and that Wassenaar itself has never been used to mitigate human-rights concerns before. Nonetheless I acknowledge that the EU has decided to use these instruments to regulate intrusion software and I was glad to read that in the motion presented by Miss Schaake to the European Parliament she advocates for the protection of security research.

I maintain that on the topic of intrusion software the biggest threat of regulation is the chilling effect it could have on legitimate, commercial or non-profit, security research. I like to quote John Lambert, Director of The Threat Intelligence Center at Microsoft, who said: "If you shame attack research, you misjudge its contribution. Offense and defense aren't peers. Defense is offense's child". To put the quote in context, it is important to realize that Information Security is both a cost center for nearly all organizations and it is also a perfect market for lemons – public security research is what has kept in the past and keeps to date a delicate system of checks and balances in place which would not otherwise exist due to the nature of the industry.

This brings me to my next point, which is: all security vendors and most of the software vendors in general have a marked incentive in making security research illegal or taxing for the researchers. Barnaby Jack, one of the most talented and respected security researchers, wrote in 1999:

> “It is of no great surprise that attempts to outlaw reverse engineering are currently in the works, but the effects of such a proposal would be disastrous. Despite the fact that it is an open invitation for vendors to use sub-standard coding practice, there are those in the security industry who rely on these techniques to find and document vulnerabilities. The online world would suffer as a result. Do not concede. ”.

It seems to me that Barnaby Jack was correct ten years ago as he is today, unfortunately. Recently, high-profile companies such as Oracle, Fireeye and Bluecoat have all used legal means to try and coerce researchers into silence to avoid the publication of flaws found in the company products.

The proposal developed by my colleagues and myself aims at two goals, the first one is to render regulation more effective in actually curbing the sale of surveillance software and the second is to ensure that legitimate research is still possible without inconvenience or the need to apply for an export license. The proposals here forth are not mutually exclusive and could be combined as the regulator sees it fit.

1. Regulate infection/injection proxies for installation at an ISP

The surveillance systems that compromise endpoints (computers and phones) all work in the same manner: A monitoring device is installed at ISP or backbone level which - through some signature such as a “marker” or “selector” - identifies the correct computer to compromise. The device then modifies or injects data into the existing data stream - in most cases, an executable that is being downloaded is being infected during the download, in some rare cases, an exploit is delivered.

This architecture is present, in almost-unchanged-form, in all the surveillance software samples publicly disclosed. The reason for this is that such an architecture represents by far the most effective way of performing endpoint intrusions: Any identifier for an individual is sufficient to attack his endpoint the next time he comes online. Traditional phishing attacks have in practice a too-low rate of success.

I would like to stress that zero-day exploits are almost never used in common off-the-shelf surveillance software (such as Gamma or Hacking Team products).

2. Regulate exfiltration software

No matter how an endpoint is compromised, a fundamental requirement of any surveillance tool is the ability to exfiltrate data from the target. Intrusion software nearly always contains a software component that sends sensitive data back to a command-and-control center operated by the owner or the buyer of the surveillance software.
The vast majority of the exfiltration software has no legitimate use and could safely be regulated without having adverse consequences on legitimate security research.

3. Create auto-triggering sanctions for regimes caught using such technology

Even if exports of such surveillance technology from within the EU to repressive regimes can be curbed, it is doubtful that the market niche will not be filled by suppliers from other countries.

In order to truly create incentives for repressive regimes to not use such technology, getting caught using it needs to have consequences *for the buy side*. This could mean suspension of economic aid, trade sanctions, or other means of imposing a cost on the use of such methods to violate the human rights of the population.

4. Change the current "whitelist" approach (that is, applying for export licenses for a broadly-defined good) into a more careful "blacklist" approach

It is common for technology companies to prevent the export of technology to so-called "T-5" countries (Crimea, Cuba, Iran, North Korea, Sudan, Syria). It should not be difficult for the EU to maintain an official list of countries known to violate human rights routinely.

The current export control implementation requires companies to by-default apply for export licenses. The burden on security researchers and companies would be greatly reduced if this "whitelist" approach was changed to a blacklist approach: Export of intrusion software either requires specific licenses or is generally not allowed for countries on the list of human rights violators - but no such restrictions exist for countries not on this list.

5. Shift the definition of "intrusion software" to focus on intent, not functionality

The problem of software that can be used in two ways (with identical feature sets) is not new - in the world of DRM and copy-protections, the same problem arose many years ago: There is legitimate need and use for backup software, but the backup software might need to circumvent a DRM mechanism in order to allow users to make legitimate backups of their data or software. At the same time, sales of DRM-circumvention software were deemed undesirable.

The problem was solved by relying on "manifest intent" - e.g. in what way is the software marketed, what are the features used to convince customers to buy the software, and so forth.

6. Establish a technical committee of Information Security Researchers

Personally I attribute the disastrous wording in the Wassenaar agreement to the lack of proper technical council, unfortunately neither privacy rights organizations nor most of the technical people within governments have the adequate knowledge needed to properly understand how intrusion software actually works and hence how to mitigate the risks it poses.

Given the delicacy of the problem it is important to select subject matter experts that have experience in writing, analyzing and defending against surveillance software to work together with policy-makers on the final implementation of the regulation.

In closing, I would like to thank my colleagues Thomas Dullien, Georg Wicherski and Stefano Zanero who couldn't be present today. I would also like to thank you once again for your time and for the opportunity to be here.