c/o Privacy International
62 Britton Street
London
EC1M 5UY
United Kingdom

23 February 2016

Dear Wassenaar Arrangement participants,

We are writing to express our concern that elements of the current control list of technologies and proposed new additions will have adverse effects on human rights and security. While we strongly support restrictions on the proliferation of surveillance technologies, we also wish to ensure that the Arrangement does not undermine cybersecurity and security research. Based on these considerations, we are writing with regard to the current language of controls on Intrusion Software, Encryption, and the proposed inclusion of Forensic Tools, and to encourage members to ensure that control text adopted through the Wassenaar Arrangement are narrowly-scoped and appropriate.

As technologies change and new ones develop, export controls need to be revisited periodically, in an open and transparent manner. We firmly believe that well-defined and strategically-chosen items should be controlled, and that even the simple outcome of tracking the exports is essential to accountability. The uncontrolled trade in advanced surveillance capabilities used for security, law enforcement, and espionage poses a serious threat to human rights – as has been demonstrated in recurrent nightmare scenarios where they have fallen into the hands of brutal regimes. Concurrently, we also believe that disproportionate and burdensome controls on tools that enhance privacy and security is also a threat to global stability, security, and the protection of human rights. The challenge is to balance these legitimate interests and narrowly-define the technologies of concern.

Subjecting certain surveillance systems to export restrictions is necessary to protect human rights. The intrusive nature of this type of monitoring and intelligence gathering – the fact that it can be used against targets located anywhere in the world – and the absence of a robust legislative framework governing their use makes these unlawful and dangerous. Widely-available evidence in the public domain shows how such products have been sold by companies and subsequently used for human rights violations.

As a result, we welcomed a number of inclusions to the controls. These include the 2012 inclusion of mobile telecommunications interception equipment (5.A.1.f), and the 2013 inclusion of IP network communications surveillance systems or equipment (5.A.1.j). Such equipment can be used for mass surveillance to indiscriminately intercept the mobile and electronic communications of thousands of individuals.

As you know, in 2013, "surveillance and law enforcement/intelligence gathering tools" were added to the dual use list, as "Systems, equipment, and components related to Intrusion Software" (4.A.5). As we have learned based on a groundswell of concerns from the information security community, often unsatisfied by clarifications from export control authorities, the current language of the control presents an onerous burden on legitimate transfers. This is a cost that is both unnecessary and disproportionate to our commonly shared objectives of enhancing national, economic, and infrastructure security.

As you are aware, the core criteria for including an item within control lists includes clear and

objective specification of the item, the ability to enforce regulations, and the minimal risk of unintended consequences. The potential for regulations within the computer and telecommunications network security context to have negative consequences upon individuals and IT security research therefore makes regulatory measures particularly challenging. The specific components of the intrusion software control provide an unfortunate example of the problems of an opaque consultation process and the challenges present as the Wassenaar Arrangement considers new technologies. For example, cybersecurity professionals have expressed fears that the "technology for development of intrusion software" control imposes licensing obligations on the discovery, disclosure and ultimate remediation of vulnerabilities. While some member states have individually sought to address or remedy some of these concerns, in capturing a broad range of common practices, regulators have been unable to allay concerns. To add onto the current pressure, we are concerned that the implementation of these new rules in national frameworks have gone beyond what is required. This has left a piecemeal fabric of interpretations and activities. The consequence of hindering the exchange of vulnerability information poses a risk to all Internet users, and subsequently creates meaningful human rights concerns. We urge participants to reflect upon this as you revisit the controls. As for the particular governments who have established expansive rules, we request that you withdraw and revisit them.

Similarly, the fact that encryption technology continues to be on the dual use list is highly inappropriate. The original intent of the encryption controls now run counter to the protection of the right to privacy, as well as international and personal security, with little benefit. As the increase of hacking incidents has demonstrated, encryption is a key means to ensure that citizens can protect their data against criminals and malicious actors. At a time in which governments are focused on cyber defenses, removing impediments to secure systems should be a priority. Similarly, the unintended consequences of export controls on information security have been severe. Indeed, some of the vulnerabilities in existing products are a direct results of the controls (see CVE-2016-0800), and software developers are commonly stifled by incomprehensible rules that have come to impede their work. Moreover, the cryptographic software available in the public domain is equivalent to those controlled by Wassenaar, leading the control to fail on foreign availability and effectiveness. We urge participants to end this long-unnecessary impediment and remove encryption technology from the control list.

Lastly, it has been speculated that participating states are currently discussing whether to include specific 'forensic tools' in the dual use list. Like Intrusion Software, certain forensic tools which can be used for surveillance of devices by law enforcement agencies and others, are also essential to enhance and improve cybersecurity. As the experience of the Intrusion Software control has shown, expertise in the information security and IT sectors is diffused across a range of different stakeholders, making effective policy-making reliant on individuals outside of national governments, including from industry, academia, and civil society. Without such consultation, we urge participating states to reject any controls on specific forensic tools.

We understand that if adequate language cannot be drafted to capture all of the above within this arrangement, then it is highly likely that this means that Intrusion Software would have to be removed from the controls list. On these grounds, Forensic Tools would have to be excluded as well.

In summation, we strongly recommend urge member states to take these considerations into account prior to final agreement and the plenary session in December 2017.

- Control language for items relating to Intrusion Software needs to be updated.
- Zero day vulnerabilities/exploits/Proof of Concepts must not come within its reach (even as an exception).
- Exceptions for security research are not adequate.
- The chilling effect of the language must also be taken into consideration.

We look forward to working with you on how we can address the serious risks these technologies may pose to human rights and international security, and appreciate your attention to the matter.

Yours sincerely,

Access Now
Chaos Computer Club (CCC)
Electronic Frontier Foundation (EFF)
European Digital Rights (EDRi)
Initiative für Netzfreiheit
IT-Political Association of Denmark
Privacy International
Vrijschrift
Collin Anderson, Independent Researcher