

# Cyber-Security Regulations Update

---

OVERVIEW OF DEVELOPMENTS IN CONTROLS

## The Wassenaar Language

---

4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of "intrusion software".

4. D. 4. "Software" specially designed or modified for the generation, command and control, or delivery of "intrusion software".

c. "Technology" for the "development" of "intrusion software"

## “Intrusion Software”

---

"Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following:

- a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
- b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

## Notes to the Definition

---

1. "Intrusion software" does not include any of the following:
  - a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;
  - b. Digital Rights Management (DRM) "software"; or
  - c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.
2. Network-capable devices include mobile devices and smart meters.

---

#### Technical Notes

1. 'Monitoring tools': "software" or hardware devices, that monitor system behaviours or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.
2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing

## US Perspective

---

Cyber threats move at Internet speed and so must cyber responders, to protect networks and data across the globe. Imagine the impact on cybersecurity if responders, innovators, and developers were told to pause and apply for an export license before responding to a threat. With a new round of international negotiations about to begin for the Wassenaar Arrangement, now is the time to press hard to arrive at a workable international standard that protects, rather than undermines, cybersecurity.



## Issues Identified

“Unfortunately, the approach proposed by the Wassenaar regulation misses the mark, and indeed, the controls would ultimately undermine that goal by making it harder for cyber responders to defend against the use of surveillance technologies. Because the regulation is so overly broad, it would require cyber responders and security researchers to obtain an export license prior to exchanging essential information to remediate a newly-identified network vulnerability, even when that vulnerability is capable of being exploited for purposes of surveillance. It would also require an onerous licensing process for sales of strong cybersecurity tools and services by companies around the world, and in some cases, could prohibit their sale altogether.”

<https://www.steptoecyberblog.com/2017/02/15/cybersecurity-and-the-wassenaar-arrangement-what-needs-to-be-done-in-2017/>

## Questions & Discussion

---

