41 Nations Meet to Review Changes to the Wassenaar Arrangement

Details of the Wassenaar Arrangement and Its Influence on Technology

What is the Wassenaar Arrangement?

- An agreement between 41 nations **to limit the export of military-grade weapons**
- Formed in light of the end of the Cold War, the agreement sought to mitigate the risk to international security brought on by the development **of large-scale munitions** due to advances in technology
- A 2013 amendment **added internet-based surveillance systems** in the list of restricted exports in order to prevent Western tech companies from selling surveillance software to governments that abuse human rights

Why Does It Matter to the Tech World?

- **Zero-days** are bugs in software unknown to the user or developer that can be exploited to damage or gain access to a system; they are particularly harmful because they are **undiscovered**, meaning **no protective measures** have been taken to prevent them
- The scope of the Wassenaar Agreement restrictions also covers surveillance software used by **security researchers looking to detect vulnerabilities before they can be exploited**
- Restricting the proliferation of such software can come at the expense of zero-day detection, **potentially harming companies** unknowingly using vulnerable software or are aiming to search for vulnerabilities

Sources: Sebastian Anthony, "The First Rule of Zero-Days is No One Talks about Zero-Days (So We'll Explain)," ArsTechnica, October 20, 2015; Tim Starks, "Export Controls on Cybersecurity Products Back on the Agenda," Politico, June 20, 2016; Joe Uchill, "Nations to Review Cyber Export Rules," The Hill, June 20, 2016; Noun Project, 2016.

Groups from Business, Technology, and Government Sectors Voice Opinions About the Future of the Provision

Details of Interest Groups and Next Steps

Who Has Spoken Out?

- **Cybersecurity companies** whose practices and sales are at risk
- **Tech platforms** like Google and Facebook, who rely on bug bounty programs and tools restricted by the amendment to learn about their own security, and engage in share threat intelligence with each other
- **Human rights advocates** who point out the abusive uses of this software
- Reps. **Jim Langevin** (D-RI) and **Michael McCaul** (R-TX) have urged revisions to its implementation in the US
- Delegates for the talks include representatives from the State Department, the Commerce Department, Homeland Security, and cybersecurity companies Luta Security and VMWare

What's Next?

- Talks are set to last until **Wednesday** in Vienna
- Another round of talks will take place in **September**
- A **December** plenary session will make any agreed-upon changes official, for which the State Department has listed "removal of the technology control" on the agenda

Sources: Sebastian Anthony, "The First Rule of Zero-Days is No One Talks about Zero-Days (So We'll Explain)," ArsTechnica, October 20, 2015; Tim Starks, "Export Controls on Cybersecurity Products Back on the Agenda," Politico, June 20, 2016; Joe Uchill, "Nations to Review Cyber Export Rules," The Hill, June 20, 2016; "White House Responds to Langevin and McCaul on Wassenaar Concerns," Congressman Jim Langevin, February 2, 2016; Noun Project, 2016.