ISN
ETH Zurich

31 July 2014

Exporting Surveillance: A New International Security Issue

Network surveillance systems and intrusion software were recently added to the list of conventional and dual-use technologies that are controlled under the Wassenaar Arrangement. For Tim Maurer and Robert Morgus, however, this is just the first step in regulating the growing export trade in surveillance technology.

By Tim Maurer and Robert Morgus for ISN

From the Stasi in Cold War East Germany to security forces in contemporary Syria, surveillance has long been an effective tool for authoritarian governments to root out dissent and identify potential points of unrest. Before the widespread use of the Internet and social media, domestic surveillance depended on a heavy police presence, human intelligence methods, and the occasional use of technology to bug a room or tap a wire. Today, governments are increasingly using these new technologies to collect and monitor the data and conversations of their citizens on an unprecedented scale.

Until recently, the global trade in equipment enabling electronic surveillance was largely unchecked. It first entered the spotlight after the Arab uprisings. When the archives of fallen Arab regimes opened to the public, they provided a unique insight into those regimes' inner workings and trade relationships. As a result, the French government opened a judicial inquiry into Amesys, a French company that sold surveillance technology to Gadhafi's security forces. Remnants of Blue Coat operating systems , sold by an American company, were also uncovered in Syria. This made it clear that companies in the U.S. and Europe were providing these technologies to regimes with dubious human rights records that used them against their citizens.

The global market for surveillance tools has ballooned in recent years. According to the Wall Street Journal , the retail market for these technologies "sprung up from 'nearly zero' in 2001 to around $5 billion a year" in 2011. This explosion in demand reflects the shifting dynamics of surveillance associated with the move online. While these technologies, such as Hacking Team's Remote Control System and Gamma International's FinFisher, can be useful for law enforcement purposes, they become problematic when exported to countries without the rule of law and with little respect for human rights. Recent reports even suggest that the Ethiopian government used kits supplied by European firms to spy on people living in the United States and the United Kingdom.

Countries where these companies are based, such as the United Kingdom, the U.S., Germany, and

France, are taking notice. In December 2013, the state parties to the Wassenaar Arrangement, a 41 member state export control regime, moved to restrict the export of two types of surveillance technologies. This represents the first significant attempt to govern the growing global trade in surveillance technologies

What is the Wassenaar Arrangement?

The Wassenaar Arrangement is a multilateral arms control regime and the successor of the Coordinating Committee for Multilateral Export Controls (CoCom), the principal arms control regime established by the United States and its post-War allies in the late 1940s. Throughout the Cold War, CoCom provided a forum through which the United States could coordinate with other major weapons manufacturing countries to restrict the flow of conventional arms to the Soviet Union and its Warsaw Pact allies. Controls agreed upon at CoCom then had to be ratified and implemented into domestic export control frameworks. Although CoCom ceased to function in March 1994, its regulations remained in effect under the Wassenaar Arrangement, which was established in July 1996.

The Wassenaar Arrangement is not a treaty and is therefore not legally binding under international law per se but depends on each of its members to implement the agreements domestically. Moreover, compared to CoCom, the Wassenaar Arrangement is less strict with regard to institutional veto power. Wassenaar has two lists, the Dual-Use Control List and the Munitions List. The Munitions List consists of conventional arms like missiles, tanks, and guns, while the Dual-Use List restricts items like sonar, composites and laminates, and radio equipment. The Dual-Use List also includes encryption items – products used to *evade* surveillance rather than the surveillance equipment itself.

Last December, the Wassenaar membership – which, unlike CoCom, includes Russia in addition to the United States, United Kingdom, France, and Germany – agreed to implement new controls relating to intrusion software and IP network surveillance systems. The intrusion software control affects the export of products like Gamma's FinFisher, which can be used to execute commands remotely and surreptitiously swipe passwords, screenshots, microphone recordings, camera snapshots, and Skype chats. The IP network surveillance systems control affects the sale of products like Amesys' Eagle, which can monitor general network traffic and identify and collect information flowing through a network. The current language of the update supports a control of the infrastructure for intrusion software, not of intrusion software itself and is very narrow to allow continued vulnerability research, a crucial component of computer security.

Why now?

The decision to create these new controls appears to be a response to the growing awareness and pressure regarding the surveillance trade. A Dutch Member of European Parliament, for example, publically highlighted the connection between these technologies and people who have been dragged from their homes and jailed. Human Rights Watch released an in-depth report earlier this year examining the effects of network surveillance in Ethiopia concluding that the mere presence of these devices can cause self-censorship. And a group of non-profit organizations launched the Coalition Against Unlawful Surveillance Exports Network raising awareness that network surveillance systems and intrusion software pose clear threats to the right to privacy, outlined in theUnited Nations' Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Protections, in addition to the basic freedoms of speech and assembly guaranteed by Article 19 in the Covenant [New America's Open Technology Institute, where the authors work, is a member of this coalition.]

The growing awareness and the actions taken by governments and NGOS are starting to have an effect. For example, revelations regarding the proliferation of its FinFisher malware have brought

Gamma International under intensive examination in the UK and Germany. Seeking less restriction and scrutiny, Gamma sought a license to export from Switzerland in September 2013. However, the British non-governmental organization Privacy International sent letters to the Swiss State Secretariat for Economic Affairs, calling on the president and foreign minister to "step into the debate and refuse license applications for surveillance technology that are currently awaiting approval for export out of Switzerland." As Privacy International notes, the Swiss Good Controls Act requires the refusal of licenses that violate Switzerland's international commitments, like those to the Wassenaar Arrangement. In March, Switzerland reported that all applications for the export of "technologies for internet monitoring" were withdrawn. Though the Swiss did approve the export of some cell phone monitoring equipment, statements from government officials indicate that they took human rights concerns into consideration and only allowed sales to countries that had been receiving these products for years.

While the Wassenaar Arrangement provides a multilateral mechanism to control the trade of such technologies and to deny companies the ability to shop around for favorable jurisdictions, these developments raise novel questions for American and European foreign policy. Wassenaar was originally conceived as a traditional arms control regime and does not explicitly contain considerations for human rights. Nevertheless, preventing surveillance technologies from flowing freely should make it more difficult for undemocratic regimes to monitor their citizens and consolidate power. How to align and prioritize these conflicting policy goals will be a growing challenge. Additionally, questions regarding how to monitor and control transshipment in the digital age require more research. Without a human rights component, however, the Wassenaar Arrangement cannot provide a holistic lens through which the major exporters can approach the sale of these products. The update in December was only the first step on a long road towards a comprehensive global structure to govern the surveillance trade.

For more information on issues and events that shape our world, please visit the ISN Blog or browse our resources.

Tim Maurer is a non-resident fellow at the Global Public Policy Institute (GPPi) and a research fellow at the New America Foundation's Open Technology Institute in Washington DC. Prior to joining the New America Foundation, Tim was a research associate at the Center for Strategic and International Studies, where he continues to be an adjunct fellow.

Robert Morgus is a research associate at the Open Technology Institute where he provides research and writing support on cyber space and international affairs. His work focuses on swing states in the Internet governance debate, Internet freedom in the context of U.S. export controls, technical sovereignty, and cybersecurity.

Publisher

International Relations and Security Network (ISN)
