The Information Warfare Monitor Project Publishable Summary

The Information Warfare Monitor (IWM) project closed in January 2012, having conducted advanced research activity tracking the emergence of cyberspace as a strategic domain.

The IWM was established in 2002 by Ronald Deibert from the Citizen Lab at the Munk School of Global Affairs, University of Toronto and Rafal Rohozinski from the The SecDev Group (formerly the Advanced Network Research Group, University of Cambridge, UK), as a sister project to the Open Net Initiative of which Deibert and Rohozinski are principal investigators along with John Palfrey (Berkman Center for Internet and Society, Harvard University) and Jonathan Zittrain (Oxford Internet Institute).

The research of the IWM was supported by the Canada Centre for Global Security Studies (University of Toronto), a grant from the John D. and Catherine T. MacArthur Foundation, in-kind and staff contributions from the SecDev Group, and a donation of software from Palantir Technologies Inc.

The IWM had the following three fold objectives:

- To apply an evidence-based approach to, and stimulate critical scholarly research around the study of conflict in cyberspace, including computer network warfare, cyber espionage and surveillance, and targeted malware attacks.

- To influence global cyber-security policy, and in particular encourage the development of norms of mutual restraint and cyber arms control

- To engage, educate, and assist civil society groups on cyber-security best practices

The projects main achievements include:

Original Research

- In 2008, the IWM discovered a surveillance network being operated by Skype and its Chinese Partner, TOM Online, which insecurely and routinely collected, logged, and captured millions of records (including personal information and contact details for any text chat and/or voice calls placed to TOM-Skype users, including those from the Skype platform).

- In 2009, after a 10-month investigation, the IWM discovered and named GhostNet, a suspected cyber-espionage operation, based mainly in the People's Republic of China, which has infiltrated at least 1,295 computers in 103 countries 30% of which were high-value targets, including ministries of foreign affairs, embassies, international organizations, news media, and NGOs.

- Published in 2010 is a report titled *Shadows in the Cloud: Investigating Cyber Espionage 2.0*. The IWM documented a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The investigation recovered a large quantity of stolen documents – including sensitive and classified materials – belonging to government, business, academic, and other computer network systems and other politically sensitive targets

- Also published in 2010, having discovered archived copies of the Koobface botnet's infrastructure on a well-known Koobface command and control server, IWM researchers documented the inner workings of Koobface in their 2010 report, *Koobface: Inside a Crimeware Network*. Researchers discovered that in just one year, Koobface generated over US$2million in profits.

Policy Engagement

- One of the IWMs core activities was policy engagement to promote the emergence of international norms of mutual restraint. Since its formation in 2003 the IWM pursued this objective through participation at major international meetings and forums and engagements with policy makers and practitioners across US, Canada, Russia, China, and NATO.

Civil Society Outreach

- The IWM worked closely with human rights groups and civil society actors who have been under targeted cyber-attacks. Outreach of the IWM included Tibetan communities, the Tibetan government in Exile, The Offices of His Holiness the Dalai Lama, the

Foreign Correspondents in China Club, and Burmese human rights and independent media groups. These associations were mutually beneficial: data related to their attacks is critical to our investigations and scholarly analyses; our investigations and analyses provide evidence of security vulnerabilities, threat assessments, and risk analysis.

As the IWM project has ended, the project's web site is no longer maintained and has been archived.

Thank you for your support of the IWM project over the years. If you would like to follow up with the Citizen Lab, please contact Ron Deibert at r.deibert [at] utoronto.ca, or with the SecDev Group, please contact Rafal Rohozinski at r.rohozinski [at] secdev.ca