Richard Bejtlich

Nonresident Senior Fellow, The Brookings Institution

Richard Bejtlich is a nonresident senior fellow at the Brookings Institution and an advisor to security start-ups. He was previously Chief Security Strategist at FireEye, and Mandiant's Chief Security Officer when FireEye acquired Mandiant in 2013. At General Electric, as Director of Incident Response, he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. His fourth book is "The Practice of Network Security Monitoring" (nostarch.com/nsm). He also writes for his blog (taosecurity.blogspot.com) and Twitter (@taosecurity).

Bejtlich's research focuses on integrating strategic thought into private sector cyber defense. He asserts that computer networks are best protected by adopting strategies of rapid, holistic incident detection and response, but he is investigating the extent to which that approach scales beyond the enterprise to the "Internet of Things."

Bejtlich is currently working on his master's and doctorate in philosophy in war studies at King's College London. He advises the cybersecurity start-ups Threat Stack, Sqrrl and Critical Stack.

Previously, Bejtlich served on the board of the Open Information Security Foundation and was the director of incident response for General Electric (GE), where he built and led the 40-member GE Computer Incident Response Team. Prior to GE, he operated TaoSecurity LLC as an independent consultant, protected national security interests for ManTech Corporation's Computer Forensics and Intrusion Analysis Division, investigated intrusions as part of Foundstone's incident response team, and monitored client networks for Ball Corporation. Bejtlich began his digital security career as a military intelligence officer in 1997 at the U.S. Air Force Computer Emergency Response Team, Air Force Information Warfare Center and Air Intelligence Agency.

Bejtlich has testified to the House Committee on Foreign Affairs, the House Committee on Homeland Security, the Senate Armed Services Committee, and the U.S.-China Economic and Security Review Commission. He has appeared on *Bloomberg West*, the *Nightly Business Report*, PBS *NewsHour*, CNN, *This Week in Defense News*, *The Kojo Nnamdi Show*, *To the Point*, *Federal News Radio*, and *BBC Radio*. He has been interviewed and cited by *The New York Times*, *The Wall Street Journal*, *The Washington Post*, *Forbes*, *Foreign Policy,* and other newspapers and magazines. He appeared in the 2013 documentary film *Hacked*, and won *The Economist*'s first online debate on cybersecurity. He has delivered guest lectures at the Massachusetts Institute of Technology, Georgetown University, U.S. Air Force Academy, U.S. Naval Academy, U.S. Military Academy, University of Cambridge, and other institutions. He has spoken at the Atlantic Council, Chatham House, Politico, the Center for National Policy, and other think tanks.

Bejtlich wrote *The Tao of Network Security Monitoring* (Addison-Wesley, 2004) and *Extrusion Detection: Security Monitoring for Internal Intrusions* (Addison-Wesley, 2005), and co-authored *Real Digital Forensics: Computer Security and Incident Response* (Addison-Wesley, 2005). His article "Don't Underestimate Cyber Spies: How Virtual Espionage Can Lead to Actual Destruction" appeared in *Foreign Affairs* in March 2013. He earned a Master of Public Policy from Harvard University, as well as a Bachelor of Science in history and a Bachelor of Science in political science from the United States Air Force Academy.