The U.S. Government's Secret Plans to Spy for American Corporations

Glenn Greenwald ⋮ 6-8 minutes ⋮ 9/5/2014

Throughout the last year, the U.S. government has repeatedly insisted that it does not engage in economic and industrial espionage, in an effort to distinguish its own spying from China's infiltrations of Google, Nortel, and other corporate targets. So critical is this denial to the U.S. government that last August, an NSA spokesperson emailed *The Washington Post* to say (emphasis in original): "The department does ***not*** engage in economic espionage in any domain, including cyber."

After that categorical statement to the *Post*, the NSA was caught spying on plainly financial targets such as the Brazilian oil giant Petrobras; economic summits; international credit card and banking systems; the EU antitrust commissioner investigating Google, Microsoft, and Intel; and the International Monetary Fund and World Bank. In response, the U.S. modified its denial to acknowledge that it *does* engage in economic spying, but unlike China, the spying is never done to benefit American corporations.

Director of National Intelligence James Clapper, for instance, responded to the Petrobras revelations by claiming: "It is not a secret that the Intelligence Community collects information about economic and financial matters…. What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—U.S. companies to enhance their international competitiveness or increase their bottom line."

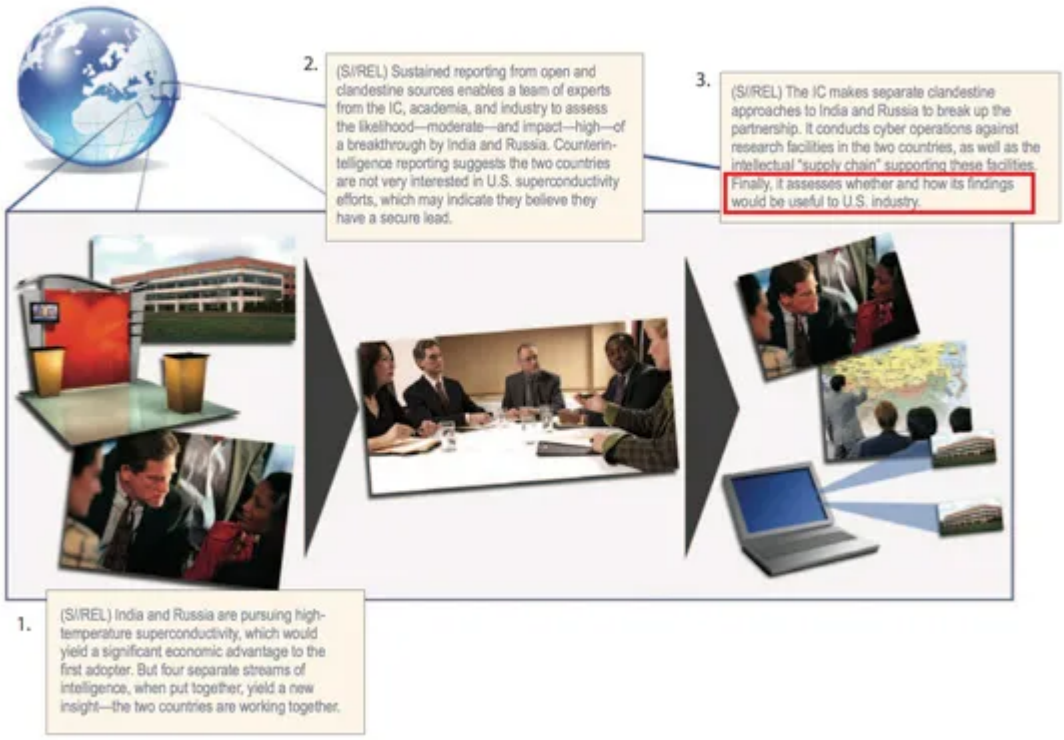
But a secret 2009 report issued by Clapper's own office explicitly contemplates doing exactly that. The document, the 2009 Quadrennial Intelligence Community Review—provided by NSA whistleblower Edward Snowden—is a fascinating window into the mindset of America's spies as they identify future threats to the U.S. and lay out the actions the U.S. intelligence community should take in response. It anticipates a series of potential scenarios the U.S. may face in 2025, from a "China/Russia/India/Iran centered bloc [that] challenges U.S. supremacy" to a world in which "identity-based groups supplant nation-states," and games out how the U.S. intelligence community should operate in those alternative futures—the idea being to assess "the most challenging issues [the U.S.] could face beyond the standard planning cycle."

One of the principal threats raised in the report is a scenario "in which the United States' technological and innovative edge slips"— in particular, "that the technological capacity of foreign multinational corporations could outstrip that of U.S. corporations." Such a development, the report says "could put the United States at a growing—and potentially permanent—disadvantage in crucial areas such as energy, nanotechnology, medicine, and information technology."

How could U.S. intelligence agencies solve that problem? The report recommends "a multi-pronged, systematic effort to gather open source and *proprietary information through overt means, clandestine penetration (through physical and cyber means)*, and counterintelligence" (emphasis added). In particular, the DNI's report envisions "cyber operations" to penetrate "covert centers of innovation" such as R&D facilities.

- **(S//REL) Cyber Operations.** The IC would sustain close-access collection, frequently by second and third parties, to non-public and/or covert centers of innovation by implanting applications (i.e., bots) that run automated tasks and sensors in software and hardware used by foreign researchers and manufacturers, and by conducting computer-network exploitation of foreign R&D intranets. In select instances, this could also involve development of long-term sources.

In a graphic describing an "illustrative example," the report heralds "technology acquisition by all means." Some of the planning relates to foreign superiority in surveillance technology, but other parts are explicitly concerned with using cyber-espionage to bolster the competitive advantage of U.S. corporations. The report thus envisions a scenario in which companies from India and Russia work together to develop technological innovation, and the U.S. intelligence community then "conducts cyber operations" against "research facilities" in those countries, acquires their proprietary data, and then "assesses whether and how its findings would be useful to U.S. industry" (click on image to enlarge):



The document doesn't describe any previous industrial espionage, a fact the DNI's office emphasized in responding to questions from *The Intercept.* A spokesman, Jeffrey Anchukaitis, insisted in an email that "the United States—unlike our adversaries—does not steal proprietary corporate information to further private American companies' bottom lines," and that "the Intelligence Community regularly engages in analytic exercises to identify potential future global environments, and how the IC could help the United States Government respond." The report, he said, "is not intended to be, and is not, a reflection of current policy or operations."

Yet the report describes itself as "an essential long-term piece, looking out between 10 and 20 years" designed to enable "the IC [to] best posture itself to meet the range of challenges it may face." Whatever else is true, one thing is unmistakable: the report blithely acknowledges that stealing secrets to help American corporations secure competitive advantage is an acceptable future role for U.S. intelligence agencies.

In May, the U.S. Justice Department indicted five Chinese government employees on charges that they spied on U.S. companies. At the time, Attorney General Eric Holder said the spying took place "for no reason other than to advantage state-owned companies and other interests in China," and "this is a tactic that the U.S. government categorically denounces."

But the following day, *The New York Times* detailed numerous episodes of American economic spying that seemed quite similar. Harvard Law School professor and former Bush Justice Department official Jack Goldsmith wrote that the accusations in the indictment sound "a lot like the kind of cyber-snooping on firms that the United States does." But U.S. officials continued to insist that using surveillance capabilities to bestow economic advantage for the benefit of a country's corporations is wrong, immoral, and illegal.

Yet this 2009 report advocates doing exactly that in the event that "that the technological capacity of foreign multinational corporations outstrip[s] that of U.S. corporations." Using covert cyber operations to pilfer "proprietary information" and then determining how it "would be useful to U.S. industry" is precisely what the U.S. government has been vehemently insisting it does not do, even though for years it has officially prepared to do precisely that.

Illustration: Getty Images