THE HILL

The new imitation game

By Patrick G. Eddington

January 8, 2015

By the time I visited America's answer to Britain's Bletchley Park codebreaking facility—NSA's sprawling obsidian headquarters at Ft. Meade—as a fledgling CIA analyst in the late1980s, signals intelligence had grown from a job for tweedy mathematicians tweaking mechanical codebreaking machines to a full-time career for tens of thousands of employees in a global network of computer-assisted listening posts. Even so, the broad outlines remained the same: making and breaking secret codes was something nation state adversaries did to each other on dedicated communications channels far removed from civilian networks.

That paradigm ended on a Tuesday morning in September 2001 when, in less than three hours, the United States suffered more casualties from a hostile attack than it had since Pearl Harbor.

Massive intelligence failures rarely provoke the kind of immediate and probing introspection necessary to establish exactly why the surprise occurred. More typically, the public outcry for revenge produces a "rally around the flag" effect, with attention deflected from the Intelligence Community's (IC) failure. Instead, we refocus our energies on giving more money and legal license to the agencies that failed to protect us.

The eventual post-mortems on the 9/11 intelligence failure produced predictable findings. The IC had more than enough data to uncover the attack but failed to "connect the dots," just like every other intelligence failure from Pearl Harbor to the present day. But those findings had zero impact on rolling back the unprecedented surveillance powers granted to the NSA in the months and years after the attacks. And as we now know, those powers were turned inward, against the American public, as much as they had been expanded outward against the amorphous and ever-changing radical Islamist threat.

In the 21st century, anyone who uses the Internet—from terrorists plotting jihad to teenagers trading cat photos—relies to some extent on encryption. And that makes us all targets.

The NSA's actions and policies are a threat to the Constitution and to the very future of the internet. Many in the privacy and civil liberties community are coming to terms with the reality that they are up against a hostile intelligence service that has used and will continue to use every means at its disposal to break open source encryption technologies. That became apparent in December 2014 when *Der Spiegel*, drawing on documents in the Snowden archive, revealed the

extent of the NSA's assault on core internet technologies and protocols used for all manner of secure communications online, including banking. While some of those technologies still appear to be viable for ordinary internet users, "hacktivists," journalists, and privacy advocates recognized they were now in a digital arms race against NSA.

NSA uses multiple tried-and-true methods to achieve its goal, from the least expensive to the most:

Legislation: The de facto legalization of mass surveillance through laws like the PATRIOT Act and the Foreign Intelligence Surveillance Amendments (FISA) Act helps NSA's overall collection process. But as we know from revelations about NSA's activities under the Reagan-era Executive Order 12333, they are just a few of the tools at NSA's disposal and not necessary ones for targeting individuals or organizations outside of the U.S., including organizations employing U.S. citizens.

Source recruitment/penetration: NSA's successful efforts to subvert the encryption standards processes at the National Institutes for Standards and Technology were documented in 2013. In late 2014, we learned of more NSA efforts to electronically or physically penetrate key global telecommunications companies and international standards organizations. The goal is always the same: find the right people who will compromise encryption keys, encryption standards, or entire networks to facilitate and maintain NSA access to all available traffic, regardless of type or mode of transmission.

Invest in new brute-force attack methods. When I worked on the U.S. Commission on Research and Development in the U.S. Intelligence Community, it became clear that NSA's obsession with certain emerging technologies was driven by a palpable sense of fear that the spread of encryption globally would cause NSA to "go dark." That obsession will continue to drive NSA's efforts for ever-larger, always secret appropriations to find the next best technology and techniques to allow it to make all communications—by foreign governments or by me and you over the internet—readable in as close to real-time as possible.

If these efforts were focused only against actual or potential enemies of the United States, Americans would strongly support it. Indeed, it was that kind of focus that allowed American military cryptographers to break key Japanese codes in the Pacific theater and British codebreakers to crack Nazi Germany's "Enigma" cypher machine in World War II, the latter achievement depicted in the 2014 movie "The Imitation Game." But the NSA's new "imitation game" threatens the very foundations of our democracy and our tech-reliant economy. Hoarding secret vulnerabilities doesn't just preserve NSA's capabilities against its adversaries, it also preserves their adversaries' capabilities against all the innocent users of cryptographic tools—including gay people like Alan Turing living in surveillance states that still consider homosexuality a crime. It's a game none of us can afford to play.

Eddington is a policy analyst in Homeland Security and Civil Liberties at the Cato Institute and a former CIA analyst.