GlobalResearch
Center for Research on Globalization

The U.S. Secret State and the Internet: “Dirty Secrets” and “Crypto Wars” from “Clipper Chip” and ECHELON to PRISM

By Tom Burghardt

Global Research, May 19, 2015
Antifascist Calling and Global Research 11 November 2013

Region: USA
Theme: Intelligence, Police State & Civil Rights

First published in November 2013

Back in the 1990s, security researchers and privacy watchdogs were alarmed by government demands that hardware and software firms build “backdoors” into their products, the millions of personal computers and cell phones propelling communication flows along the now-quaint “information superhighway.”

Never mind that the same factory-installed kit that allowed secret state agencies to troll through private communications also served as a discrete portal for criminal gangs to loot your bank account or steal your identity.

To make matters worse, instead of the accountability promised the American people by Congress in the wake of the Watergate scandal, successive US administrations have worked assiduously to erect an impenetrable secrecy regime backstopped by secret laws overseen by secret courts which operate on the basis of secret administrative subpoenas, latter day *lettres de cachet*.

But now that all their dirty secrets are popping out of Edward Snowden’s “bottomless briefcase,” we also know the “Crypto Wars” of the 1990s never ended.

Documents published by *The Guardian* and *The New York Times* revealed that the National Security Agency “actively engages the US and IT industries” and has “broadly compromised the guarantees that internet companies have given consumers to reassure them that their communications, online banking and medical records would be indecipherable to criminals or governments.”

> “Those methods include covert measures to ensure NSA control over setting of international encryption standards,” The Guardian disclosed, along with “the use of supercomputers to break encryption with ‘brute force’, and–the most closely guarded secret of all–collaboration with technology companies and internet service providers themselves.”

According to *The New York Times*, NSA “had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors or by surreptitiously exploiting existing security flaws, according to the documents."

In fact, "vulnerabilities" inserted "into commercial encryption systems" would be known to NSA alone. Everyone else, including commercial customers, are referred to in the documents as "adversaries."

The cover name for this program is Project BULLRUN. An agency classification guide asserts that "Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE [computer network exploitation], interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques."

In furtherance of those goals, the agency created a "Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with industry partners" that will "further NSA/CSS capabilities against encryption used in network communications technologies," and already "has some capabilities against the encryption used in TLS/SSL. HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communications technologies."

Time and again, beginning in the 1970s with the publication of perhaps the earliest NSA exposé by *Ramparts Magazine*, we learned that when agency schemes came to light, if they couldn't convince they resorted to threats, bribery or the outright subversion of the standard setting process itself, which destroyed trust and rendered all our electronic interactions far less safe.

Tunneling underground, NSA, telcos and corporate tech giants worked hand-in-glove to sabotage what *could* have been a free and open system of global communications, creating instead the Frankenstein monster which AT&T whistleblower Mark Klein denounced as a "Big Brother machine."

The Secret State and the Internet

Five years after British engineer Tim Berners-Lee, Belgian computer scientist Robert Cailliau and their team at CERN developed a system for assembling, and sharing, hypertext documents via the internet, which they dubbed the World Wide Web, in 1994 the Clinton administration announced it would compel software and hardware developers to install what came to known as the "Clipper Chip" into their products.

The veritable explosion of networked communication systems spawned by the mass marketing of easy-to-use personal computers equipped with newly-invented internet browsers, set off a panic amongst political elites.

How to *control* these seemingly anarchic information flows operating outside "normal" channels?

In theory at least, those doing the communicating–academics, dissidents, journalists, economic rivals, even other spies, hackers or "terrorists" (a fungible term generally meaning outsider groups not on board with America's imperial goals)–were the least amenable users of the new technology and would not look kindly on state efforts to corral them.

As new communication systems spread like wildfire, especially among the great unwashed mass of “little people,” so too came a stream of dire pronouncements that the internet was now a “critical national asset” which required close attention and guidance.

President Clinton’s Commission on Critical Infrastructure Protection released a report that called for a vast increase in funding to protect US infrastructure along with one of the first of many “cyberwar” tropes that would come to dominate the media landscape.

“In the cyber dimension,” the report breathlessly averred, “there are no boundaries. Our infrastructures are exposed to new vulnerabilities–cyber vulnerabilities–and new threats–cyber threats. And perhaps most difficult of all, the defenses that served us so well in the past offer little protection from the cyber threat. Our infrastructures can now be struck directly by a variety of malicious tools.”

And when a commercial market for cheap, accessible encryption software was added to the mix, security mandarins at Ft. Meade and Cheltenham realized the genie would soon be out of the bottle.

After all they reasoned, NSA and GCHQ were the undisputed masters of military-grade cryptography who had cracked secret Soviet codes which helped “win” the Cold War. Were they to be out maneuvered by some geeks in a garage who did not share or were perhaps even hostile to the “post-communist” triumphalism which had decreed America was now the world’s “indispensable nation”?

Technological advances were leveling the playing field, creating new democratic space in the realm of knowledge creation accessible to everyone; a new mode for communicating which threatened to bypass entrenched power centers, especially in government and media circles accustomed to a monopoly over the Official Story.

US spies faced a dilemma. The same technology which created a new business model worth hundreds of billions of dollars for US tech corporations also offered the public and pesky political outliers across the political spectrum, the means to do the same.

How to stay ahead of the curve? Why not control the tempo of product development by crafting regulations, along with steep penalties for noncompliance, that all communications be accessible to our guardians, strictly for “law enforcement” purposes mind you, by including backdoors into commercially available encryption products.

Total Information Awareness 1.0

Who to turn to? Certainly such hush-hush work needed to be in safe hands.

The Clinton administration, in keeping with their goal to “reinvent government” by privatizing everything, turned to Mykotronx, Inc., a California-based company founded in 1983 by former NSA engineers, Robert E. Gottfried and Kikuo Ogawa, mining gold in the emerging information security market.

Indeed, one of the firm’s top players was Ralph O’Connell, was described in a 1993 document published by Computer Professionals for Social Responsibility (CPSR) as “the father of COMSEC” and the “Principle NSA Technical Contact” on Clipper and related cryptography projects.

A 1993 Business Wire release quoted the firm’s president, Leonard J. Baker, as saying that

Clipper was "a good example of the transfer of military technology to the commercial and general government fields with handsome cost benefits. This technology should now pay big dividends to US taxpayers."

It would certainly pay "big dividends" to Mykotronx's owners.

Acquired by Rainbow Technologies in 1995, and eventually by Military-Industrial-Surveillance Complex powerhouse Raytheon in 2012, at the time the *Los Angeles Times* reported that "Mykotronx had been privately held, and its owners will receive 1.82 million shares of Rainbow stock–making the deal worth $37.9 million."

The Clipper chip was touted by the administration as a simple device that would protect the private communications of users while also allowing government agents to obtain the keys that unlocked those communications, an early manifestation of what has since become know as law enforcement's alleged "going dark" problem.

Under color of a vague "legal authorization" that flew in the face of the 1987 Computer Security Act (CSA), which sought to limit the role of the National Security Agency in developing standards for civilian communications systems, the administration tried an end-run around the law through an export ban on Clipper-free encryption devices overseen by the Commerce Department.

This wasn't the first time that NSA was mired in controversy over the watering down of encryption standards. During the development of the Data Encryption Standard (DES) by IBM in the 1970s, the agency was accused of forcing developers to implement changes in the design of its basic cipher. There were strong suspicions these changes had weakened the algorithm to such a degree that one critical component, the S-box, had been altered and that a backdoor was inserted by NSA.

Early on, the agency grasped CSA's significance and sought to limit damage to global surveillance and economic espionage programs such as ECHELON, exposed by British and New Zealand investigative journalists Duncan Campbell and Nicky Hager.

Before the 1987 law was passed however, Clinton Brooks, a Special Assistant to NSA Director Lieutenant General William Odom, wrote a Top Secret Memorandum which stated: "In 1984 NSA engineered a National Security Decision Directive, NSDD-145, through the Reagan Administration that gave responsibility for the security of all US information systems to the Director of NSA, removing NBS [National Bureau of Standards] from this."

Conceived as a follow-on to the Reagan administration's infamous 1981 Executive Order 12333, which trashed anemic congressional efforts to rein-in America's out-of-control spy agencies, NSDD-145 handed power back to the National Security Agency and did so to the detriment of civilian communication networks.

Scarcely a decade after Senator Frank Church warned during post-Watergate hearings into government surveillance abuses, that NSA's "capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter . . . there would be no place to hide," the agency was at it with a vengeance.

"This [NSDD-145] also stated," Brooks wrote, "that we would assist the private sector. This was viewed as Big Brother stepping in and generated an adverse reaction" in Congress that helped facilitate passage of the Act.

Engineered by future Iran-Contra felon, Admiral John Poindexter, President Reagan's National Security Adviser who would later serve as President George W. Bush's Director of DARPA's Information Awareness Office, the Pentagon satrapy that brought us the Total Information Awareness program, NSDD-145 stated that the "Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security."

NSA's new mandate meant that the agency would "act as the government focal point for cryptography, telecommunications systems security, and automated information systems security."

Additionally, NSA would "conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information."

But it also authorized the agency to do more than that, granting it exclusive authority to "review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security." As well, NSA was directed to "enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies, where appropriate, to private organizations, including government contractors, and foreign governments."

In other words, NSA was the final arbiter when it came to setting standards for *all* government and private information systems; quite a coup for the agency responsible for standing-up Project MINARET, the Cold War-era program that spied on thousands of antiwar protesters, civil rights leaders, journalists and members of Congress, as recently declassified documents published by the National Security Archive disclosed.

NSA Games the System

Although the Computer Security Act passed unanimously by voice vote in both Houses of Congress, NSA immediately set-out to undercut the law and did so by suborning the National Bureau of Standards, now the National Institute of Standards and Technology (NIST).

The battle over the Clipper Chip would be the template for future incursions by the agency for the control, through covert infiltration, of regulatory bodies overseeing civilian communications.

According to the Clinton White House, Clipper "would provide Americans with secure telecommunications without compromising the ability of law enforcement agencies to carry out legally authorized wiretaps."

Neither safe nor secure, Clipper instead would have handed government security agencies the means to monitor all communications while giving criminal networks a leg up to do the same.

In fact, as the Electronic Privacy Information Center (EPIC) discovered in documents unearthed through the Freedom of Information Act, the underlying algorithm deployed in Clipper, Skipjack, had been developed by NSA.

Cryptography expert Matt Blaze wrote a now famous 1994 paper on the subject before the algorithm was declassified, *Protocol Failure in the Escrowed Encryption Standard*: "The EES cipher algorithm, called 'Skipjack', is itself classified, and implementations of the cipher are available to the private sector only within tamper-resistant modules supplied by government-approved vendors. Software implementations of the cipher will not be possible. Although Skipjack, which was designed by the US National Security Agency (NSA), was reviewed by a small panel of civilian experts who were granted access to the algorithm, the cipher cannot be subjected to the degree of civilian scrutiny ordinarily given to new encryption systems."

This was precisely as NSA and the Clinton administration intended.

A partially declassified 1993 NSA memo noted that "there will be vocal public doubts expressed about having a classified algorithm in the device we propose for the US law enforcement problem, the CLIPPER chip, we recommend the following to address this." We don't know what those agency recommendations were, however; more than 20 years after the memo was written they remain secret.

The memo continued: "If such people agree to this clearance and non disclosure process, we could go over the algorithm with them to let them develop confidence in its security, and we could also let them examine the detail design of the CLIPPER chip made for the US law enforcement problem to assure themselves that there were no trapdoors or other techniques built in. This would likely require crypto-mathematicians for the algorithm examination and microelectronics chip design engineers for the chip examination."

But the extreme secrecy surrounding Skipjack's proposed deployment in commercial products *was* the problem. Even if researchers learned that Clipper was indeed the government-mandated backdoor they feared, non-disclosure of these facts, backed-up by the threat of steep fines or imprisonment would hardly assure anyone of the integrity of this so-called review process.

"By far, the most controversial aspect of the EES system," Blaze wrote, "is key escrow."

> "As part of the crypto-synchronization process," Blaze noted, "EES devices generate and exchange a 'Law Enforcement Access Field' (LEAF). This field contains a copy of the current session key and is intended to enable a government eavesdropper to recover the cleartext."
>
> "The LEAF copy of the session key is encrypted with a device-unique key called the 'unit key,' assigned at the time the EES device is manufactured. Copies of the unit keys for all EES devices are to be held in 'escrow' jointly by two federal agencies that will be charged with releasing the keys to law enforcement under certain conditions."

What those conditions were however, was far from clear. In fact, as we've since learned from Snowden's cache of secret documents, even when the government seeks surveillance authorization from the FISA court, the court must rely on government assurances that dragnet spying is critical to the nation's security. Such assurances, FISA court judge Reggie B. Walton noted, were systematically "misrepresented" by secret state agencies.

That's rather rich considering that Walton presided over the farcical "trial" that upheld Bush administration demands to silence FBI whistleblower Sibel Edmonds under the state secrets privilege. Edmonds, a former contract linguist with the Bureau charged that top FBI officials had systematically covered-up wrongdoing at its language division and had obstructed agents' attempts to roll-up terrorist networks *before* and *after* the 9/11 provocation, facts attested to by FBI whistleblower Coleen Rowley in her 2002 Memo to then-FBI Director Robert Mueller.

In 2009, Walton wrote that "The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively."

"The Court," Walton averred, "must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. The Court no longer has such confidence."

Predating those critical remarks, a heavily-redacted 1993 Memo to then-Special Assistant to the President and future CIA chief, George Tenet, from FBI Director William Sessions noted that NSA "has developed a new encryption methodology and computer chip which affords encryption strength vastly superior to DES [Digital Encryption Standard], yet which allows for real time decryption by law enforcement, acting pursuant to legal process. It is referred to as 'Clipper'."

[Two redacted paragraphs] "if the devices are modified to include the 'Clipper' chip, they would be of great value to the Federal, state and local law enforcement community, especially in the area of counter narcotics, investigations, where there is a requirement to routinely communicate in a secure fashion."

But even at the time Sessions' memo was written, we now know that AT&T provided the Drug Enforcement Administration "routine access" to "an enormous AT&T database that contains the records of decades of Americans' phone calls," *The New York Times* reported, and had done so since 1987 under the auspices of DEA's Hemisphere Project.

Furthermore, in the wake of Snowden revelations we also learned that listening in on the conversations of drug capos is low on NSA's list of priorities. However, programs like X-KEYSCORE and TEMPORA, which copies all data flowing along fiber optic cables, encrypted and unencrypted alike, at petabyte scales, is supremely useful when it comes to building profiles of internet users by intelligence agencies.

This was an implicit goal of Clinton administration maneuvers to compel developers to insert Clipper into their product designs.

According to Sessions, "the 'Clipper' methodology envisions the participation of three distinct types of parties." [Redacted] It is proposed that the second party, the two custodians of the 'split' key infostructure [sic], be comprised of two disinterested and trustworthy non law enforcement Government agencies or entities. Although, such decision and selection are left for the Administration, a list of reccommended [sic] agencies and entities has been prepared (and included in the text), [redacted]. This party would administer and oversee all facets of the 'Clipper' program and methodology."

Based on NSDD-145's mandate, one can assume "this party" would be NSA, the agency that designed the underlying algorithm that powered Clipper.

The Sessions memo averred: "The Clipper chip provides law enforcement access by using a special chip key, unique to each device. In the AT&T TSD 3600, a unique session key is generated, external to the Clipper chip for each call."

> "This session key," the memo explained, "is given to the chip to control the encryption algorithm. A device unique 'chip key' is programmed into each Clipper at the time of manufacture. When two TSD 3600s go to secure operation, the device gives out its identification (ID) number and the session key encrypted in its chip key."

Underlining a key problem with Clipper technology Sessions noted, "Anyone with access to the chip key for that identified device will be able to recover the session key and listen to the transmission simultaneously with the intended receiver. This design means that the list of chip keys associated with the chip ID number provides access to all Clipper secured devices, and thus the list must be carefully generated and protected. Loss of the list would preclude legitmate [sic] access to the encrypted information and compromise of the list could allow unauthorized access."

In fact, that "anyone" could include fabulously wealthy drug gangs or bent corporations with the wherewithal to buy chip keys from suborned government key escrow agents!

Its ubiquity would be a key selling-point for universal deployment. The memo explained, "the NSA developed chip based 'Clipper' solution works with hardware encryption applications, such as those which might be used with regard to certain telecommunications and computers devices," which of course would allow unlimited spying by "law enforcement."

Such vulnerabilities built into EES chip keys *by design* not only enabled widespread government monitoring of internet and voice traffic, but with a few tweaks by encryption-savvy "rogues" could be exploited by criminal organizations.

In his 1994 paper Blaze wrote that "a rogue system can be constructed with little more than a software modification to a legal system. Furthermore, while some expertise may be required to install and operate a rogue version of an existing system, it is likely that little or no special skill would be required to install and operate the modified software."

"In particular," Blaze noted, "one can imagine 'patches' to defeat key escrow in EES-based systems being distributed over networks such as the Internet in much the same way that other software is distributed today."

In the intervening years since Blaze observed how easy it would be to compromise key escrow systems by various bad actors, governments or criminals take your pick, the proliferation of malware powered botnets that infect hundreds of thousands of computers and smart phones every day–for blanket surveillance, fraud, or both–is a fact of life.

It didn't help matters when it emerged that "escrow agents" empowered to unlock encrypted communications would be drawn from the National Institute of Standards and Technology and the Automated Services Division of the Treasury Department, government outposts riddled with "No Such Agency" moles.

As EPIC pointed out, "Since the enactment of the Computer Security Act, the NSA has sought to undercut NIST's authority. In 1989, NSA signed a Memorandum of Understanding (MOU) which purported to transfer back to NSA the authority given to NIST."

The MOU required that NIST request NSA's "assistance" on all matters related to civilian cryptography. In fact, were NIST and NSA representatives on the Technical Working Group to disagree on standards, the ultimate authority for resolving disputes would rest solely with the Executive Branch acting through the President, the Secretary of Defense and the National Security Council, thus undercutting the clear intent of Congress when they passed the 1987 Computer Security Act.

EPIC noted:

> "The memorandum effectively returned to NSA many of the powers rejected by the Computer Security Act. The MOU contained several key goals that were to NSA's benefit, including: NSA providing NIST with 'technical security guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data;' NSA 'initiating research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods'; and NSA being responsive to NIST 'in all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement'."

A critique of the Memorandum in 1989 congressional testimony by the General Accounting Office (GAO) emphasized: "At issue is the degree to which responsibilities vested in NIST under the act are being subverted by the role assigned to NSA under the memorandum. The Congress, as a fundamental purpose in passing the act, sought to clearly place responsibility for the computer security of sensitive, unclassified information in a civil agency rather than in the Department of Defense. As we read the MOU, it would appear that NIST has granted NSA more than the consultative role envisioned in the act."

Five years after the GAO's critical appraisal, NSA's coup was complete.

"In 1994," EPIC noted,

> "President Clinton issued Presidential Decision Directive (PDD-29). This directive created the Security Policy Board, which has recommended that all computer security functions for the government be merged under NSA control."

Since PDD-29 was issued matters have only gotten worse. In fact, NIST is the same outfit exposed in Snowden documents published by *The Guardian* and *The New York Times* that allowed NSA to water down encryption and build backdoors into the Dual EC DRBG standard adopted by the Institute in 2006.

"Eventually, NSA became the sole editor."

Besieged by widespread opposition, the Clinton administration was out maneuvered in the court of public opinion and by 1996 had abandoned Clipper. However, this proved to be a pyrrhic victory for security-minded researchers and civil libertarians as we have since learned from Edward Snowden's revelations.

Befitting a military-intelligence agency, the dark core of America's deep state, NSA was fighting a long war–and they were playing for keeps.

The original source of this article is Antifascist Calling and Global Research

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Tom Burghardt**
http://antifascist-calling.blogspot.com/

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca