



and then published same. The defense has the right to rebut that claim by cross-examining any expert proffered by the government and by calling its own expert. In both circumstances, the defense requires discovery in order to make that case. The discovery sought here is solely within the possession of the United States and is exculpatory.

As set forth in the Indictment, and as is set forth in 18 U.S.C. § 793, one of the elements of all of these counts is the requirement that the information disclosed be “related to the national defense” and information that “could be used to the injury of the United States or to the advantage of a foreign power.” Similarly, in its recent Motion in *Limine* Seeking to Admit the Testimony of James Risen, the government states over and over again that Mr. Risen will testify that Mr. Sterling disclosed “national defense information” to him and that the “national defense information” was then published. (Govt’s Mot. in Lim., p. 20.)

Courts, regardless of the ease with which the government makes these allegations, have struggled to define “national defense information” especially in cases involving alleged leaks to reporters. To that end, in overruling constitutional challenges to charges under 18 U.S.C. § 793 (d) and (e), courts have held that “information relating to the national defense” is legally limited to information that is closely held by the United States government, and that the information is the type which, if disclosed, could threaten the national security of the nation. United States v. Rosen, 445 F. Supp. 2d 602, 621 (E.D.Va. 2006) (citing United States v. Morison, 844 F.2d 1057, 1071-72 (4th Cir. 1985)(“disclosure would be potentially damaging to the United States or useful to an enemy of the United States.”)).

Here, all that is before the Court is a certain chapter of a book that contains Mr. Risen’s

recitation of what he purports to have learned about certain events. The government has attached the applicable chapter of that book, State of War, to its Motion in *Limine* Seeking to Admit the Testimony of James Risen as Exhibit A. The government does not contend that the entire book or even a single complete chapter contains “national defense information.” It therefore necessarily leaves to the jury and the Court the issue of determining whether the information allegedly disclosed legally qualifies as “national defense information.” In that regard, because this case deals with an alleged leak to a reporter of “national defense information,” this case is quite different from past cases when the information at issue was tangible and specific such as war plans, budget plans or satellite photographs.

The Morison case is illustrative of the type of information that is usually at issue in one of these cases.<sup>1</sup> The defendant in Morison had stolen classified photographs depicting a Soviet aircraft carrier under construction in a naval shipyard in the Black Sea. Morison, 844 F.2d at 1061. In that case, the government successfully argued that the photographs were harmful to the interests of the United States and provided an advantage to the Soviet Union. Id. at 1061. The photograph was tangible evidence that could be unarguably tied to that defendant through fingerprints and a typewriter ribbon. Id. at 1062. In fact, in many cases prosecuted under 18 U.S.C. § 793, the national defense information that at issue is tangible evidence. See Rosen, 445 F. Supp. 2d at 614, fn. 8 (citing United States v. Poulsen, 41 F. 3d 1330, 1333 (9th Cir. 1994) (charged with the willful retention of stolen computer tapes containing air tasking orders); United

---

<sup>1</sup> Mr. Sterling is not charged with disclosing classified information to anyone not entitled to receive it. The statute of limitations on such a charge ran long ago.

States v. Pollard, 959 F.2d 1011, 1015-16 (4th Cir. 1992) (transmission of photocopied documents to Israeli intelligence services); United States v. Zetl, 835 F.2d 1059, 1060 (4th Cir. 1987) (delivery of classified Navy documents); United States v. Walker, 796 F.2d 43, 45 (4th Cir. 1986) (transmittal of Navy documents containing classified information to the Soviet Union); United States v. Troung Dinh Hung, 629 F.2d 908, 911-12 (4th Cir. 1980) (transmission of documents relating to the national defense to Socialist Republic of Vietnam during the 1977 Paris peace negotiations); United States v. Kampiles, 609 F.2d 1233, 1235 (7th Cir. 1980) (delivery of a military technical manual to the Soviet Union); United States v. Lee, 589 F.2d 980, 982-83 (9th Cir. 1999) (transmittal of documents relating to a covert communications satellite study to the Soviet Union); United States v. Doe, 455 F.2d 1270, 1272 (1st Cir. 1972) (transmittal of the "Pentagon Papers" published by the Washington Post and New York Times); United States v. Ntube, 1996 U.S. Dist. LEXIS 20617, No. 93-0322-2 (D.D.C. 1996) (delivery of classified documents to certain African countries).

The defense cites these cases not to show that tangible national defense information is a necessary element of a charge under 18 U.S.C. § 793. This exact argument was found to be unpersuasive in Rosen and is not here repeated. But a tangible piece of information is easily identified and defined. The jury can decide, apparently with the assistance of expert testimony<sup>2</sup>

---

<sup>2</sup> The defense anticipates that the government will rely upon expert testimony in order to seek to prove the disclosure of "national defense information." The Court has imposed no schedule as to when that expert disclosure must be made. The defense notes that such disclosure must be made sufficiently in advance of the trial that an opposing expert can be cleared and review the report in order to develop his or her expert report and testimony. As of this date, the defense has no information or report of any form about any potential expert for the government on this critical issue.

from both sides, whether it fits the criteria of national defense information the unauthorized disclosure of which is tantamount to espionage. Here, the information at issue must be considered in the form in which the alleged disclosure has made itself to the public record since that is the form of the alleged publication of the "national defense information." And this issue is made more complicated because the government, as is shown in more detail below, claims that at least some of the information that was disclosed is false. This fact also complicates the discovery issue before the Court because it cannot be a crime to disclose false "national defense information" since false information would not fit the statutory definition. For example, the disclosure of false information, such as phony budget numbers or forged "Pentagon Papers," could not be damaging to the United States or advantageous to one of its enemies. Since the defense does not know what factual information, if any, in Chapter 9 of State of War is true or false, it is incumbent upon the government to answer those questions and provide discovery as to what actually took place and what did not. The defense has sought this information without the intervention of the Court to no avail.

**2. The Alleged Disclosures in State of War.**

In the Indictment in this case there are numerous allegations that Mr. Sterling schemed to get Mr. Risen to publish the "national defense information" that is set forth in State of War. In response to an Order requiring a Bill of Particulars, and then as Exhibit A to its Motion in *Limine* Seeking to Admit the Testimony of James Risen, the government identified the information at issue as somewhere set forth in certain pages of Chapter 9 of State of War. In short, Chapter Nine tells a story of an alleged effort undertaken by the CIA to provide false blueprints for a

component of a nuclear weapon to the Iranians in 1999 and 2000. Mr. Risen wrote:

[T]he CIA believed that once the Iranians had the blueprints and studied them, they would believe the designs were usable and so would start to build an atom bomb based upon the flawed designs. But Tehran would get a big surprise when its scientists tried to explode their new bomb. Instead of a mushroom cloud, the Iranian scientists would witness a disappointing fizzle. The Iranian nuclear program would suffer a humiliating setback, and Tehran's goal of becoming a nuclear power would have been delayed by several years. In the meantime, the CIA, by watching Iran's reaction to the blueprints, would have gained a wealth of information about the status of Iran's weapons program, which had been shrouded in secrecy.

State of War, p. 209.

The fact alone that the United States is opposed to the Iranian nuclear weapons program is no secret. Nor is it a secret that the United States and its allies have taken many steps to delay or stop the Iranian nuclear program. Hardly a day passes when some story is not published regarding the Iranian nuclear program and the efforts of Israel or the United States to stop it. Recently, multiple press outlets released stories of a "worm" or computer virus had infected computer at the Iranian nuclear plants and that the "worm" had been delivered somehow by the United States.<sup>3</sup> A recent example of such a story was published in the New York Times. (*"Israeli Test on Worm Called Crucial in Iran Nuclear Delay,"* William J. Broad, David E. Sanger, John Markoff, New York Times, January 15, 2011)("Exhibit A"). Here is an example of just how "closely held" the idea that the United States and Israel are seeking to delay Iranian nuclear ambitions and are taking actions in that regard:

---

<sup>3</sup> The defense has no information as to whether any fact or statement in this story is true or false but provides it to the Court to show how prevalent in the media re reports on this topic. This is a very small sampling of a large amount of public information.

The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.

The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. Nor is it clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults . . . .

The project's political origins can be found in the last months of the Bush administration. In January 2009, The New York Times reported that Mr. Bush authorized a covert program to undermine the electrical and computer systems around Natanz, Iran's major enrichment center. President Obama, first briefed on the program even before taking office, sped it up, according to officials familiar with the administration's Iran strategy. So did the Israelis, other officials said. Israel has long been seeking a way to cripple Iran's capability without triggering the opprobrium, or the war, that might follow an overt military strike of the kind they conducted against nuclear facilities in Iraq in 1981 and Syria in 2007.

Two years ago, when Israel still thought its only solution was a military one and approached Mr. Bush for the bunker-busting bombs and other equipment it believed it would need for an air attack, its officials told the White House that such a strike would set back Iran's programs by roughly three years. Its request was turned down. . . . .

Id.

In order to prosecute this case, the government will have to show that the "national defense information" it relies upon is actually true. And, it will have to show just how the publication or dissemination of that information aided Iran or some other enemy of the United States. At a minimum, it must allow the defense to challenge the accuracy of that testimony by confronting the witnesses called by the government with the truth of what actually occurred.

From reading Chapter Nine, it is impossible for the defense to know what, if anything,

actually happened in Vienna or Iran or anywhere else as described in State of War. It is impossible to know whether the blueprints that were allegedly provided were ever received in the first place or then used by the Iranian in the manner that Mr. Risen described above in a manner that damages the Iranian nuclear program. Again, Mr. Risen, in the book, states that he has no such information and neither does the defense. "It is not known whether the Russian ever communicated again with the Iranians, or whether they tried to contact him. But after receiving his letter warning them that they would need further help to make the blueprints useful, it is entirely possible that the Iranians showed the plans to other experts familiar with Russian nuclear designs and thereby identified the defects." State of War, pp. 211-12. Indeed, in the book itself, there is no statement that the Iranians ever received the blueprints in the first place much less used them in any way the assisted or undermined the Iranian nuclear effort. It is certainly acceptable for a journalist to argue that events are "entirely possible" to have occurred. That is not, however, the standard in a criminal case in which the defense is entitled to test the government's claim that "national defense information" was somehow disclosed by telling the jury the truth about what actually occurred and how, if at all, the alleged disclosure of the information in State of War aided the Iranians.

In this case, the defendant is entitled to tell the jury what actually happened by using the government's own evidence as that is the sole repository of that exculpatory evidence. After all, Mr. Sterling has not worked at the CIA for eleven years. In addition to details of the alleged operation, the defense is entitled to know if, as a result of the publication of State of War, the identity of Human Asset No. 1 was learned by any foreign power at all. It is entitled to know if



because of the publication of State of War, the Iranians shelved plans to use the blue prints that they allegedly learned, due to the publication of State of War, were allegedly flawed. The defense is entitled to know if this "Rogue Operation," as described by Mr. Risen, did help the Iranian nuclear program in any way. The defense, stated more broadly, must be able to use the specific facts related to this program to rebut any generic or hypothetical suggestion that any damage was done to national security by the publication of Mr. Risen's book. It has been over 6 years since Mr. Risen's book was published and 9 years since the alleged disclosure occurred. The CIA and the United States government must know what, if any damage, actually was done by publication of the book. Indeed, it cannot be believed that the government has not conducted a full investigation as to the alleged consequences of these disclosures. The government is obligated to produce that information in time for a defense expert to review and for a full CIPA process allowing for the use of that evidence to occur before trial.

This issue is complicated further by the government's refusal to concede that any item of information set forth in Chapter 9 is even true. (See Govt's Mot. in Lim., p. 20, fn. 11) ("The Indictment alleges that some of the information that appears in Risen's book is national defense information - and thus is implicitly true - but also notes that some of the information contained therein is characterized in a false and misleading manner."); see also Ind. ¶¶ 18, 19 (d) ("The government is not here either confirming or denying the accuracy of any particular fact reported in the book."). It is difficult to believe that the government can show the criminal disclosure of "national defense information" without proving the accuracy of the same information. Stated in reverse, it cannot be a crime to disclose information that is false. This is, after all, not a

defamation case and falsity is a defense.


From a discovery standpoint, there are therefore substantial areas of information that are requested as exculpatory and discoverable. These items are set forth below:

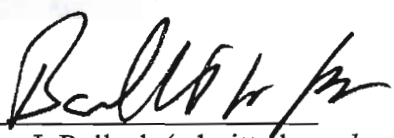
1. Any evidence of any sort that would show that the government's ability to use or deploy Human Asset No. 1 for any operation whatsoever was compromised in any way by the disclosures alleged to be at issue in this case. This request would necessarily include evidence of any operations or other assignments that Human Asset No. 1 worked on after the publication of State of War.
2. Any evidence of any sort that as a result of the publication of State of War any person or entity, or enemy of the United States, ever learned the true identity or location of Human Asset No 1 or that said person was ever in any danger at all as a result of the publication.
3. Evidence as to whether the Government has any evidence that anyone from the Iranian mission or anyone affiliated with the government of Iran ever received the package that State of War claims was allegedly dropped off. Since the Indictment alleges violations of 18 U.S.C. § 793, it would be exculpatory if the operation failed or otherwise did not accomplish the specific purposes for which it was designed. Therefore, we request all evidence of what occurred to the knowledge of the United States after the package was delivered. This would include but not be limited to any use by the Iranian government of any of the materials that were allegedly provided and whether those materials were useful to them in any way. This request would include information that as a result of the publication of State of War, the Iranians stopped building any weapon based upon that disclosure.
4. Discovery that indicates or demonstrates that any item in Chapter 9 is false.
5. Any assessment, written or oral, of the damage allegedly done to national security by the publication of State of War.
6. Any expert witness report of any expert for the United States as to the issue of "national defense information." This request would include any information discoverable as part of expert witness disclosures under Rule 16 (G) of the Federal Rules of Criminal Procedure and Rules 702, 703 or 705 of the Federal

Rules of Evidence.

Dated: June 21, 2011

JEFFREY A. STERLING  
By counsel


By:   
Edward B. MacMahon, Jr. (VSB #25432)  
Law Office of Edward B. MacMahon, Jr.  
107 E. Washington Street, P.O. Box 25  
Middleburg, VA 20118  
(540) 687-3902  
[ebmjr@verizon.net](mailto:ebmjr@verizon.net)

By:   
Barry J. Pollack (admitted *pro hac vice*)  
Miller & Chevalier Chartered  
655 Fifteenth St. N.W. Suite 900  
Washington, D.C. 20005  
(202) 626-5830  
[bpollack@milchev.com](mailto:bpollack@milchev.com)

*Counsel for Jeffrey A. Sterling*

**CERTIFICATE OF SERVICE**

I hereby certify that on June 14, 2011, I caused an electronic copy of Defendant's  
CISO  
Motion for Discovery to be served via ~~ECF~~ upon William W. Welch, II, James L. Trump, United  
States Attorney's Office.

By:   
Edward B. MacMahon, Jr. (VSB #25432)  
*Counsel for Jeffrey A. Sterling*

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS Subscribe: Home Delivery / Digital Log In Register Now Help

The New York Times

# Middle East

Search All NYTimes.com

Orange Home Loans  
As low as 3.05% APR

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS

AFRICA AMERICAS ASIA PACIFIC EUROPE MIDDLE EAST



Find the experts you need to create an environment you'll love.

FIND A PROFESSIONAL

Benjamin Moore



Advertise on NYTimes.com

## Israeli Test on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER  
Published: January 15, 2011

*This article is by William J. Broad, John Markoff and David E. Sanger.*

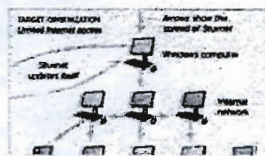
Enlarge This Image



Nicholas Roberts for The New York Times

Ralph Langner, an independent computer security expert, solved Stuxnet.

### Multimedia



Graphic

How Stuxnet Spreads

### Related

Times Topics: Stuxnet | Israel | Iran

Enlarge This Image

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not destroy, Tehran's ability to make its first nuclear arms.

RECOMMEND

TWITTER

SIGN IN TO E-MAIL

PRINT

REPRINTS

SHARE



Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This? [Log In With Facebook](#)

### What's Popular Now

Pundit Under Protest



In Italy, Voters Deliver a Rebuke to Berlusconi



## & ANALYSIS

Bloomberg GOVERNMENT BGOV.COM

Advertise on NYTimes.com

### MOST POPULAR

E-MAILED BLOGGED SEARCHED VIEWED

1. Paul Krugman: Medicare Saves Money
2. David Brooks: Pundit Under Protest
3. Seattle, a Tasting Menu
4. Ross Douthat: The Online Looking Glass
5. Profiles in Science | Nora D. Volkow: A General in the Drug War
6. Who's Ready for Kindergarten?
7. Op-Ed Contributor: Don't Quit This Day Job
8. Race Remixed : On College Forms, a Question of Race, or Races, Can Perplex
9. This Life: 'You Look Great' and Other Lies
10. Practical Traveler: How to Avoid Credit Card Problems Abroad

Go to Complete List »



President Mahmoud Ahmadinejad of Iran toured the Natanz plant in 2008.

“To check out the worm, you have to know the machines,” said an American expert on nuclear intelligence. “The reason the worm has been effective is that the Israelis tried it out.”

Though American and Israeli officials refuse to talk publicly about what goes on at Dimona, the operations there, as well as related efforts in the United States, are among the newest and strongest clues

suggesting that the virus was designed as an American-Israeli project to sabotage the Iranian program.

In recent days, the retiring chief of Israel’s Mossad intelligence agency, Meir Dagan, and Secretary of State Hillary Rodham Clinton separately announced that they believed Iran’s efforts had been set back by several years. Mrs. Clinton cited American-led sanctions, which have hurt Iran’s ability to buy components and do business around the world.

The gruff Mr. Dagan, whose organization has been accused by Iran of being behind the deaths of several Iranian scientists, told the Israeli Knesset in recent days that Iran had run into technological difficulties that could delay a bomb until 2015. That represented a sharp reversal from Israel’s long-held argument that Iran was on the cusp of success.

The biggest single factor in putting time on the nuclear clock appears to be Stuxnet, the most sophisticated cyberweapon ever deployed.

In interviews over the past three months in the United States and Europe, experts who have picked apart the computer worm describe it as far more complex — and ingenious — than anything they had imagined when it began circulating around the world, unexplained, in mid-2009.

Many mysteries remain, chief among them, exactly who constructed a computer worm that appears to have several authors on several continents. But the digital trail is littered with intriguing bits of evidence.

In early 2008 the German company Siemens cooperated with one of the United States’ premier national laboratories, in Idaho, to identify the vulnerabilities of computer controllers that the company sells to operate industrial machinery around the world — and that American



**Look out for hidden 401(k) fees**  
 ALSO IN BUSINESS »  
 A financial toolkit for women  
 A guilty trading paradox

**nytimes.com** BUSINESS

ADVERTISEMENTS

**NYTIMES.COM STYLE** Get to know J.Lo. - NYTimes.com/Style

The New York Times  
**Save 50% on home delivery** ▶

The NEW **WTOP.com**  
 Washington's 24/7 Online Source for News, Traffic & Weather

Advertise on NYTimes.com

Ads by Google what's this?

**Telstra Recharge Offer**  
 Want to Win a XOOM™ Tablet?  
 Recharge Your Pre-Paid Online Today  
[www.telstra.com.au/Prepaid-Recharge](http://www.telstra.com.au/Prepaid-Recharge)

intelligence agencies have identified as key equipment in Iran's enrichment facilities.

Siemens says that program was part of routine efforts to secure its products against cyberattacks. Nonetheless, it gave the Idaho National Laboratory — which is part of the Energy Department, responsible for America's nuclear arms — the chance to identify well-hidden holes in the Siemens systems that were exploited the next year by Stuxnet.

The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.

The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. Nor is it clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults.

"It's like a playbook," said Ralph Langner, an independent computer security expert in Hamburg, Germany, who was among the first to decode Stuxnet. "Anyone who looks at it carefully can build something like it." Mr. Langner is among the experts who expressed fear that the attack had legitimized a new form of industrial warfare, one to which the United States is also highly vulnerable.

Officially, neither American nor Israeli officials will even utter the name of the malicious computer program, much less describe any role in designing it.

But Israeli officials grin widely when asked about its effects. Mr. Obama's chief strategist for combating weapons of mass destruction, Gary Samore, sidestepped a Stuxnet question at a recent conference about Iran, but added with a smile: "I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."

In recent days, American officials who spoke on the condition of anonymity have said in interviews that they believe Iran's setbacks have been underreported. That may explain why Mrs. Clinton

provided her public assessment while traveling in the Middle East last week.

By the accounts of a number of computer scientists, nuclear enrichment experts and former officials, the covert race to create Stuxnet was a joint project between the Americans and the Israelis, with some help, knowing or unknowing, from the Germans and the British.

The project's political origins can be found in the last months of the Bush administration. In January 2009, The New York Times reported that Mr. Bush authorized a covert program to undermine the electrical and computer systems around Natanz, Iran's major enrichment center. President Obama, first briefed on the program even before taking office, sped it up, according to officials familiar with the administration's Iran strategy. So did the Israelis, other officials said. Israel has long been seeking a way to cripple Iran's capability without triggering the opprobrium, or the war, that might follow an overt military strike of the kind they conducted against nuclear facilities in Iraq in 1981 and Syria in 2007.

Two years ago, when Israel still thought its only solution was a military one and approached Mr. Bush for the bunker-busting bombs and other equipment it believed it would need for an air attack, its officials told the White House that such a strike would set back Iran's programs by roughly three years. Its request was turned down.

Now, Mr. Dagan's statement suggests that Israel believes it has gained at least that much time, without mounting an attack. So does the Obama administration.

For years, Washington's approach to Tehran's program has been one of attempting "to put time on the clock," a senior administration official said, even while refusing to discuss Stuxnet. "And now, we have a bit more."

### **Finding Weaknesses**

Paranoia helped, as it turns out.

Years before the worm hit Iran, Washington had become deeply worried about the vulnerability of the millions of computers that run everything in the United States from bank transactions to the power grid.

Computers known as controllers run all kinds of industrial machinery. By early 2008, the Department of Homeland Security



had teamed up with the Idaho National Laboratory to study a widely used Siemens controller known as P.C.S.-7, for Process Control System 7. Its complex software, called Step 7, can run whole symphonies of industrial instruments, sensors and machines.

The vulnerability of the controller to cyberattack was an open secret. In July 2008, the Idaho lab and Siemens teamed up on a PowerPoint presentation on the controller's vulnerabilities that was made to a conference in Chicago at Navy Pier, a top tourist attraction.

"Goal is for attacker to gain control," the July paper said in describing the many kinds of maneuvers that could exploit system holes. The paper was 62 pages long, including pictures of the controllers as they were examined and tested in Idaho.

In a statement on Friday, the Idaho National Laboratory confirmed that it formed a partnership with Siemens but said it was one of many with manufacturers to identify cybervulnerabilities. It argued that the report did not detail specific flaws that attackers could exploit. But it also said it could not comment on the laboratory's classified missions, leaving unanswered the question of whether it passed what it learned about the Siemens systems to other parts of the nation's intelligence apparatus.

The presentation at the Chicago conference, which recently disappeared from a Siemens Web site, never discussed specific places where the machines were used.

But Washington knew. The controllers were critical to operations at Natanz, a sprawling enrichment site in the desert. "If you look for the weak links in the system," said one former American official, "this one jumps out."

Controllers, and the electrical regulators they run, became a focus of sanctions efforts. The trove of State Department cables made public by WikiLeaks describes urgent efforts in April 2009 to stop a shipment of Siemens controllers, contained in 111 boxes at the port of Dubai, in the United Arab Emirates. They were headed for Iran, one cable said, and were meant to control "uranium enrichment cascades" — the term for groups of spinning centrifuges.

Subsequent cables showed that the United Arab Emirates blocked the transfer of the Siemens computers across the Strait of Hormuz to Bandar Abbas, a major Iranian port.

Only months later, in June, Stuxnet began to pop up around the globe. The Symantec Corporation, a maker of computer security

software and services based in Silicon Valley, snared it in a global malware collection system. The worm hit primarily inside Iran, Symantec reported, but also in time appeared in India, Indonesia and other countries.

But unlike most malware, it seemed to be doing little harm. It did not slow computer networks or wreak general havoc.

That deepened the mystery.

### A 'Dual Warhead'

No one was more intrigued than Mr. Langner, a former psychologist who runs a small computer security company in a suburb of Hamburg. Eager to design protective software for his clients, he had his five employees focus on picking apart the code and running it on the series of Siemens controllers neatly stacked in racks, their lights blinking.

He quickly discovered that the worm only kicked into gear when it detected the presence of a specific configuration of controllers, running a set of processes that appear to exist only in a centrifuge plant. "The attackers took great care to make sure that only their designated targets were hit," he said. "It was a marksman's job."

For example, one small section of the code appears designed to send commands to 984 machines linked together.

Curiously, when international inspectors visited Natanz in late 2009, they found that the Iranians had taken out of service a total of exactly 984 machines that had been running the previous summer.

But as Mr. Langner kept peeling back the layers, he found more — what he calls the "dual warhead." One part of the program is designed to lie dormant for long periods, then speed up the machines so that the spinning rotors in the centrifuges wobble and then destroy themselves. Another part, called a "man in the middle" in the computer world, sends out those false sensor signals to make the system believe everything is running smoothly. That prevents a safety system from kicking in, which would shut down the plant before it could self-destruct.

"Code analysis makes it clear that Stuxnet is not about sending a message or proving a concept," Mr. Langner later wrote. "It is about destroying its targets with utmost determination in military style."

This was not the work of hackers, he quickly concluded. It had to be the work of someone who knew his way around the specific quirks of

the Siemens controllers and had an intimate understanding of exactly how the Iranians had designed their enrichment operations.

In fact, the Americans and the Israelis had a pretty good idea.

### Testing the Worm

Perhaps the most secretive part of the Stuxnet story centers on how the theory of cyberdestruction was tested on enrichment machines to make sure the malicious software did its intended job.

The account starts in the Netherlands. In the 1970s, the Dutch designed a tall, thin machine for enriching uranium. As is well known, A. Q. Khan, a Pakistani metallurgist working for the Dutch, stole the design and in 1976 fled to Pakistan.

The resulting machine, known as the P-1, for Pakistan's first-generation centrifuge, helped the country get the bomb. And when Dr. Khan later founded an atomic black market, he illegally sold P-1's to Iran, Libya, and North Korea.

The P-1 is more than six feet tall. Inside, a rotor of aluminum spins uranium gas to blinding speeds, slowly concentrating the rare part of the uranium that can fuel reactors and bombs.

How and when Israel obtained this kind of first-generation centrifuge remains unclear, whether from Europe, or the Khan network, or by other means. But nuclear experts agree that Dimona came to hold row upon row of spinning centrifuges.

"They've long been an important part of the complex," said Avner Cohen, author of "The Worst-Kept Secret" (2010), a book about the Israeli bomb program, and a senior fellow at the Monterey Institute of International Studies. He added that Israeli intelligence had asked retired senior Dimona personnel to help on the Iranian issue, and that some apparently came from the enrichment program.

"I have no specific knowledge," Dr. Cohen said of Israel and the Stuxnet worm. "But I see a strong Israeli signature and think that the centrifuge knowledge was critical."

Another clue involves the United States. It obtained a cache of P-1's after Libya gave up its nuclear program in late 2003, and the machines were sent to the Oak Ridge National Laboratory in Tennessee, another arm of the Energy Department.

By early 2004, a variety of federal and private nuclear experts assembled by the Central Intelligence Agency were calling for the United States to build a secret plant where scientists could set up the

P-1's and study their vulnerabilities. "The notion of a test bed was really pushed," a participant at the C.I.A. meeting recalled.

The resulting plant, nuclear experts said last week, may also have played a role in Stuxnet testing.

But the United States and its allies ran into the same problem the Iranians have grappled with: the P-1 is a balky, badly designed machine. When the Tennessee laboratory shipped some of its P-1's to England, in hopes of working with the British on a program of general P-1 testing, they stumbled, according to nuclear experts.

"They failed hopelessly," one recalled, saying that the machines proved too crude and temperamental to spin properly.

Dr. Cohen said his sources told him that Israel succeeded — with great difficulty — in mastering the centrifuge technology. And the American expert in nuclear intelligence, who spoke on the condition of anonymity, said the Israelis used machines of the P-1 style to test the effectiveness of Stuxnet.

The expert added that Israel worked in collaboration with the United States in targeting Iran, but that Washington was eager for "plausible deniability."

In November, the Iranian president, Mahmoud Ahmadinejad, broke the country's silence about the worm's impact on its enrichment program, saying a cyberattack had caused "minor problems with some of our centrifuges." Fortunately, he added, "our experts discovered it."

The most detailed portrait of the damage comes from the Institute for Science and International Security, a private group in Washington. Last month, it issued a lengthy Stuxnet report that said Iran's P-1 machines at Natanz suffered a series of failures in mid- to late 2009 that culminated in technicians taking 984 machines out of action.

The report called the failures "a major problem" and identified Stuxnet as the likely culprit.

Stuxnet is not the only blow to Iran. Sanctions have hurt its effort to build more advanced (and less temperamental) centrifuges. And last January, and again in November, two scientists who were believed to be central to the nuclear program were killed in Tehran.

INSIDE NYTIMES.COM

The man widely believed to be responsible for much of Iran's program, Mohsen Fakrizadeh, a college professor, has been hidden away by the Iranians, who know he is high on the target list.

Publicly, Israeli officials make no explicit ties between Stuxnet and Iran's problems. But in recent weeks, they have given revised and surprisingly upbeat assessments of Tehran's nuclear status.

"A number of technological challenges and difficulties" have beset Iran's program, Moshe Yaalon, Israel's minister of strategic affairs, told Israeli public radio late last month.

The troubles, he added, "have postponed the timetable."

*This article has been revised to reflect the following correction:*

**Correction: January 17, 2011**

*An earlier version of this story misspelled, at one point, the name of the German company whose computer controller systems were exploited by the Stuxnet computer worm. It is Siemens, not Seimens.*

A version of this article appeared in print on January 16, 2011, on page A1 of the New York edition.

Connect with The New York Times on Facebook.

SIGN IN TO E-MAIL

PRINT

REPRINTS

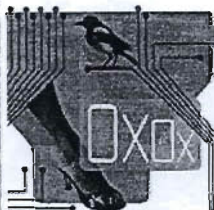
Ads by Google what's this?

**Father's Day Pants Sale**  
Get Dad Something He Will Wear!  
Save Up To 25%. Free Shipping.  
[savane.com/Mens-Pants](http://savane.com/Mens-Pants)

Get Free E-mail Alerts on These Topics

- Israel
- Iran
- Cyberattacks and Cyberwarfare
- Nuclear Weapons

HEALTH »



OPINION »

**Op-Ed: A Head-Spinning Music Festival**

Bonnaroo features a

BUSINESS »



A City Tries to Slim Down

THEATER »



OPINION »

**Fixes: The Playground Movement**

For 15 years, a group has been organizing citizens to turn their public

N.Y. / REGION »

