GlobalResearch
Center for Research on Globalization

Preemptive Policing & the National Security State: Repressing Dissent at the Republican National Convention

By Tom Burghardt
Global Research, November 19, 2008
Antifascist Calling... 18 November 2008

Region: USA
Theme: Police State & Civil Rights
In-depth Report: U.S. Elections

Antifascist Calling…

With "preemptive policing" all the rage in Washington, the whistleblowing website ***Wikileaks*** has done it again, exposing how repressive trends in the U.S. had real world consequences for democracy during September's Republican National Convention (RNC) in St. Paul, Minnesota.

On November 15, the global whistleblowers published a leaked planning **document** "Special Event Planning: 2008 Republican National Convention," a dense schematic used by repressors who targeted activists, journalists and concerned citizens during the far-right conclave.

Labeled "Limited Distribution/For Official Use Only," *Wikileaks* believes that the dossier is "potentially legally significant due to upcoming legal cases over the mass arrests at the convention."

Compiled by Terri Smith (terri.smith@state.mn.us) the Branch Director for Response, Recovery and Mitigation at the Minnesota Homeland Security and Emergency Management agency (**HSEM**), the 31-page file offers a veritable bird's-eye view onto the close coordination amongst federal, state and local law enforcement agencies, including the Pentagon's U.S. Northern Command (NORTHCOM) during a so-called National Special Security Event (NSSE).

The enabling authority for squelching dissent during NSSEs is partially derived from the 2006 National Security Presidential Directive-46/Homeland Security Presidential Directive-15 (NSPD-46/HSPD-15), a top secret dictate from President Bush.

According to a **statement** by Roger Rufe, Director of the Office of Operations Coordination and Planning (OPS) at the Department of Homeland Security (DHS), before the House Homeland Security Committee on July 9, 2008, NSSEs "are significant domestic or international events, occurrences, contests, activities, or meetings, which, by virtue of their profile or status, represent a significant target, and therefore warrant additional preparation, planning, and mitigation efforts. The designation process for NSSEs is established by NSPD-46/HSPD-15, Annex II and HSPD-7."

Rufe goes on to describe the "mission" of an NSSE Special Event Working Group (SEWG) as one which will

> …support a unified interagency planning and coordination effort for Special Events and to ensure coordination of Federal support to the designated event. The SEWG identifies events that may require a coordinated Federal response and collectively coordinates Federal assets to bridge any capability gaps identified by state and local partners that have not already been addressed by exhausting local mutual assistance agreements. Within this process, the mission of OPS is to act on behalf of the Secretary and his HSPD-5 responsibilities to integrate DHS and interagency planning and coordinate operations for designated Special Events in order to prevent, protect, respond to and recover from terrorist threats/attacks. (Roger Rufe, "Statement," House Homeland Security Committee, July 8, 2008, pp. 1-2)

Several elements comprise the SEWG: five senior managers from DHS' OPS, the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the DHS Office of Risk Management & Analysis (RMA) and, as revealed in the *Wikileaks* document, representatives from the Pentagon's U.S. Northern Command.

During the RNC, the "lead federal agencies" heading up repressive operations were the USSS, FBI and FEMA. On Saturday, August 30, 2008, the Ramsey County Sheriff's Department executed search warrants on three houses. According to the **Friends of the RNC 8**, the police seized personal items and arrested eight **RNC Welcoming Committee** organizers, charging them with "conspiracy to riot in the 2nd degree in the furtherance of terrorism," a felony which may land these activists in prison for many years under provisions of Minnesota's PATRIOT Act.

During the RNC, operations were coordinated by the Multi-Agency Communications Center (MACC), described in the *Wikileaks* file as "a centralized communications and coordination center operated 24 hours a day during the NSSE."

In St. Paul, the MACC was "staffed by representatives from all participating operational security entities, local government operations, and public and private institutions who are responsible for the critical infrastructures of power, gas and telecommunications."

MACC's "Work Product," according to the document (p. 14), will provide: "Timely dissemination of information to all entities participating in operational security, crisis management, and consequence management. Provide the Common Operational Picture to support decision-making and command and control activities," and "serve as the centralized coordination center for security-related activities."

Described as "the coordination point where these resources could be used for a crisis or consequence outside of the NSSE," the MACC was the organizational hub and speartip where federal, state, local law enforcement and "private institutions" interacted "at any time during the event to utilize the event's public safety resources to assure that the normal delivery of public safety responses from their agency were uninterrupted."

A perusal of the "MACC Seating Chart" (p. 16) affords additional insight into the resources brought to bear against journalists covering the RNC and citizens protesting the crimes of the Republican party and their Bushist minions.

The first tier is comprised of the Minneapolis Police Department (MPD), Minnesota Department of Transportation (MN DOT), Minnesota State Police (MSP), Hennepin County,

Ramsey County, St. Paul Police Department (SPPD), USSS and the FBI.

The second tier, in addition to representatives from the Minneapolis and St. Paul Fire Departments and Emergency Medical Service personnel, are staffed by three representatives from NORTHCOM. Additional NORTHCOM "seats" appear on the "third tier" of the HSEM chart, along with proxies from the Minnesota National Guard's Joint Task Force (JTF-MN), FEMA, USSS and the FBI.

MACC's fourth tier was staffed by a host of federal law enforcement entities including officers from the ultra-spooky National Geospatial-Intelligence Agency (NGA). As I have documented in several articles, most **recently** on November 9, NGA provides mapping tools and imagery intelligence (IMINT) derived from America's fleet of military spy satellites "flown" by the National Reconnaissance Office (NRO). In other words during the RNC, America's spymasters were providing satellite intelligence to federal, state, and local law enforcement, some of which quite possibly, were used to target the homes of activists and media workers or coordinate attacks on demonstrations.

While there is no indication in the MACC "seating chart" that the National Security Agency (NSA) was directly involved in providing "lead federal agencies" with signals intelligence (SIGINT), the fifth tier reveals that U.S. telecoms, all of whom are NSA private partners in warrantless wiretapping and driftnet data-mining were "present and accounted for" during the RNC.

Indeed, prominent places "at the table" were filled by Verizon Communications, Verizon Wireless, QWEST, Sprint and AT&T. Attorneys involved in defending the RNC 8 and other protesters "preemptively" arrested, would be well-advised to subpoena these company's records and determine whether or not corporate telecoms handed SIGINT over to federal, state and local repressors.

The *Wikileaks* dossier also reveals that Saint Paul Operations Center Command Posts were staffed by an entity labeled "other federal." Here one finds the FBI's Joint Operations Center (JOC) and the Bureau's Intelligence Operations Center (IOC).

Both entities have been linked during NSSEs and the surreptitious surveillance of Americans to privacy-killing FBI "packet sniffing" operations formally called Carnivore (DCS-1000). Now called Red Hook or DCS-3000, software installed on America's telephone, internet and wireless infrastructure can monitor all of a target's internet, wireless and text messaging traffic. Digital Storm, or DCS-6000, captures and collects the content of phone calls and text messages, while Magic Lantern is a keystroke surveillance tool that can be installed remotely via viral e-mail attachments. *Wired* **reported** in 2007, that Magic Lantern is a "computer and internet protocol address verifier or CIPAV," one that

> …gathers a wide range of information, including the computer's IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; preferred internet browser and version; the computer's registered owner and registered company name; the current logged-in user name and the last-visited URL.

The CIPAV then settles into a silent "pen register" mode, in which it lurks on the target computer and monitors its internet use, logging the IP address of every computer to which

the machine connects for up to 60 days. (Kevin Poulsen, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats," *Wired*, July 18, 2007)

According to **documents** released to the Electronic Frontier Foundation (**EFF**) under a Freedom of Information Act lawsuit in 2007, the Minneapolis Field Office was one of 57 sites for the Bureau's collection of "post-cut through dialed digit information." Technological heavy-lifting originated from the FBI's Science & Technology Law Unit, Engineering Research Facility located in Quantico, Virginia.

As security expert, whistleblower and CEO of Bat Blue Corporation Babak Pasdar disclosed in a sworn **affidavit** to the Government Accountability Office (GAO) back in February, Verizon Communications allowed the Bureau and other security agencies virtually "unfettered" access to the carrier's wireless network via the FBI's so-called "Quantico circuit."

Collectively, these highly-intrusive (and patently illegal) FBI programs are called DCSNet, an acronym for Digital Collection System Network. As *Wired* **revealed** in 2007, DCSNet "connects FBI wiretapping rooms to switches controlled by traditional land-line operators, internet-telephony providers and cellular companies. It is is far more intricately woven into the nation's telecom infrastructure than observers suspected."

The profound interconnections amongst federal security agencies such as the FBI and the nation's private telecoms acting in concert with securocrats is but *one* indicator of the breadth and scope of America's high-tech corporatist police state. *Wired* reports,

> The network allows an FBI agent in New York, for example, to remotely set up a wiretap on a cell phone based in Sacramento, California, and immediately learn the phone's location, then begin receiving conversations, text messages and voicemail pass codes in New York. With a few keystrokes, the agent can route the recordings to language specialists for translation.
>
> The numbers dialed are automatically sent to FBI analysts trained to interpret phone-call patterns, and are transferred nightly, by external storage devices, to the bureau's Telephone Application Database, where they're subjected to a type of data mining called link analysis.
>
> FBI endpoints on DCSNet have swelled over the years, from 20 "central monitoring plants" at the program's inception, to 57 in 2005, according to undated pages in the released documents. By 2002, those endpoints connected to more than 350 switches. (Ryan Singel, "Point, Click … Eavesdrop: How the FBI Wiretap Net Operates," Wired, August 29, 2007)

Last week, the American Civil Liberties Union (**ACLU**) revealed that the FBI no longer feels compelled to obtain judicial oversight or even the consent of cell phone operators when deploying base station-faking technology that it employs for the illegal geolocation of mobile users.

Known as Triggerfish, **documents** obtained by the ACLU in a Freedom of Information Act lawsuit against the Justice Department, detail how the technology pretends to be a cellular base station to which handsets connect and identify themselves. By claiming to have "lost" the unique identifier of a targeted mobile phone, Triggerfish then "asks" the phone to resend its unique details.

It had been assumed that a warrant was necessary before the Bureau could begin tracking an individual's cell phone. However, as the ACLU clearly reveals in the documents, under provisions of the USA Patriot Act, the FBI has been able to obtain dodgy pen-trap orders from all-too-compliant judges on the FISA court. During the RNC, these signals were probably routed via Triggerfish to the JOC/IOC: game over for "Text Mob" protest organizers.

When federal, state and local law enforcement entities raided the homes of activists and media workers in St. Paul, the Bureau knew which activists and which computers, cell phones and other electronic devices to preemptively seize.

On August 30, 2008, the FBI were joined by some 30 St. Paul police armed with tasers, pepper spray and automatic weapons when they surrounded the house where **I-Witness Video** and Democracy Now! journalist Elizabeth Press were meeting.

People inside were forcibly detained and photographed, while police made a record of the journalists' names and addresses. A warrant was served, covering all the journalist's equipment, including privileged notes, computers, cameras, video tapes and communications equipment.

Five other members of I-Witness Video who were not present during the home invasion were detained for more than three hours, preventing them from documenting three other simultaneous raids in Minneapolis and St. Paul. Additionally, members of the **Glass Bead Collective** were also illegally detained and had their notes and equipment confiscated by the Minneapolis police.

The *Wikileaks* document also reveals that the Defense Department's Joint Task Force Minnesota (JTF-MN) was a key player in the St. Paul Command Operations Center. Indeed, Major Jon Dotterer, the Operations Officer attached to JTF-MN documented in a Power Point **presentation**, "As many of you may have scene [sic] on the news the MN National Guard was used in support of the St Paul Police Department at the Republican National Convention. Our QRF [Quick Reaction Force] was used to give the local police forces the flexibility and freedom to use their assets at other critical points of interest."

Dotterer's briefing details how JTF-MN "coordinates with civil authorities," primarily HSEM, and "provides [a] response element" and "activates for [a] major contingency." What Dotterer doesn't reveal is that JTF-MN is also an active component of U.S. Northern Command.

To conclude, the *Wikileaks* document provides new and startling information how federal, state and local law enforcement entities acting in concert with corporatist "private partners" during September's Republican National Convention, conspired to deny American's their right to peacefully protest against the far-right Republican party.

With resources drawn from the FBI, USSS, DHS, NGA, FEMA and NORTHCOM, the repressive capitalist state coordinated its response to oppositional currents in the U.S. by launching preemptive attacks on RNC protest organizers and journalists.

Fully in step with the "countersubversive" mind-set underpinning the Bushist "war on terror," one that equates dissent with terrorism, recourse to preemptive policing by our corporatist masters is indicative of the precarious state of a system facing total crisis as it stares into an abyss of its creation.

Tom Burghardt *is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and* ***Global Research****, His articles can also be read on* ***Dissident Voice****,* ***The Intelligence Daily*** *and* ***Pacific Free Press****. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by* ***AK Press****.*

The original source of this article is Antifascist Calling...
Copyright © Tom Burghardt, Antifascist Calling..., 2008

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

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca