

National Security Working Group
Weekly National Security Working Group Update
Congressman Jim Jordan (R-OH), RSC Chairman
Congressman Trent Franks (R-AZ), NSWG Chairman
9 March 2011

The National Security Working Group (NSWG) is comprised of Trent Franks, 2nd, AZ; Connie Mack, 14th, FL; Duncan Hunter, 52nd, CA and Allen West, 22nd, FL. We look forward to providing RSC members updates on national security issues and matters using this forum. We welcome your inputs.

In This Newsletter:

- *Iran's Cyber Army (Rep Franks)*
 - *Chavez and Ahmadinejad: Venezuela's Sanction-Busting Activity (Rep Mack)*
 - *Fairness for Military Recruiters Act (Rep Hunter)*
 - *Electric Infrastructure Council (EIS) Summit - 11 April 2011 - Washington DC (Rep Franks)*
-

Iran's Cyber Army (Rep Franks)

The Islamic Republic of Iran is recruiting hackers who support their goals. The Iranian Cyber Army has been responsible in bringing down numerous websites recently for supposedly acting against the Islamic Republic. It is unclear whether or not the Iranian Cyber Army is affiliated with the Iranian Revolutionary Guard (IRGC). The purpose of the Cyber Army is to thwart any damage to the cultural-social infrastructure of the country. It could be used as a means for Iran's government to counter the "enemy's soft war" against the Islamic Republic. If the Iranian government is employing hackers inside the country to dismantle opposition websites, it is only a matter of time before these hackers reach the United States' infrastructure. Iran's government cyber weapons arsenal consists of: electromagnetic pulse weapons (non-nuclear), compromised counterfeit computer software, wireless data communications jammers, computer viruses and worms, cyber data collection exploits, computer and network reconnaissance tools, and embedded Trojan time bomb (suspected). It is estimated that the IRGC's cyber warfare budget is \$76 million dollars. Hackers have demonstrated their capability by successfully attacking various Israeli websites.

As reported by DefenseTech and Radio Free Europe, sources inside of Iran's Cyber Army have confirmed the existence of the hacking group and the ever-growing paranoia of the Iranian regime. It has been reported that the Twitter website was hacked by the group for fear of the blogging service was being used as a tool for Iranian prodemocracy forces. It is time for countries to start talking about the threat of a cyber war and what measures can be taken to prevent it. Cyberspace has become a new domain in warfare and with the ever more reliance on computer systems linked to the Internet; the attack in this domain could be very serious. Nobody knows for sure the true power of cyber-weapons and their secrecy makes them highly unstable.

NSWG Contact: Drew Nishiyama, Drew.Nishiyama@mail.house.gov or 5-4576 in Rep Franks' office

Chavez and Ahmadinejad: Venezuela's Sanction-Busting Activity (Rep Mack)

A key component of the United States' nuclear deterrent strategy is the enforcement of sanctions against Iran. The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010

(CISADA) is the best tool to date possessed by the U.S. to prevent Iran's Mahmoud Ahmadinejad from obtaining a nuclear weapon. CISADA has slowed, but not stopped, Ahmadinejad in his quest for nuclear technology and is constantly looking for loopholes and allies to assist him in working around sanctions. The Iranian leader has found a willing and able friend in Venezuela's Hugo Chavez whose banks have helped to bypass sanctions by providing third-party institutional support to funnel money around normal channels to sanctioned organizations. Recent reports also contain documents that show Venezuela's state-owned oil corporation Petroleos de Venezuela, S.A. (PDVSA) sending gasoline shipments to Iran that would make CISADA applicable. It is clear that Venezuela's relationship with Iran is detrimental to U.S. nuclear deterrent strategy with potentially grave implications for our national security. The Administration needs to be held accountable and enforce CISADA.

NSWG Contact: Kristin Jackson, kristin.jackson@mail.house.gov, or 5-2536 in Rep Mack's office

Fairness for Military Recruiters Act (Rep Hunter)

Recent developments with regard to Reserve Officer Training Corps (ROTC) at America's elite colleges and universities-Columbia, Yale, and until last weekend, Harvard-have reignited the debate over the denial of a student's opportunity to participate in ROTC on campus. Some of these institutions have restricted any ROTC presence since the Vietnam War. Many of these same institutions, fueled by new elements of anti-military activism, continue to deny students the opportunity to a career in the military or even consider the educational benefits and life experiences that are unique to military experience. While ROTC programs face obstacles at institutions of higher learning, the Armed Services have faced similar roadblocks at America's high schools.

Last week Mr. Hunter introduced H.R. 637, the Fairness for Military Recruiters Act. This legislation reaffirms and strengthens existing federal law. In 2002 the No Child Left Behind Act provided military recruiters the same access to high school campuses and basic student contact information provided to institutions of higher learning. Yet nine years later there are still school administrators that liberally interpret this provision and activist groups that find creative ways to restrict military recruiters. This act will ensure that military recruiters continue to have access to student information, similar to colleges, universities and other organizations recruiting students; place decisions regarding a student's personal information and future career opportunities firmly in control of his or her parents, unless a student is 18 years of age; make clear that no process other than that of a written parental request shall be used to authorize the withholding of basic student contact information; and prevent the implementation of an "opt-in" process, whereby all student information would be withheld from military recruiters.

NSWG Contact: Jimmy Thomas, jimmy.thomas@mail.house.gov in Rep Hunter's office

Electric Infrastructure Council (EIS) Summit - 11 April 2011 - Washington DC (Rep Franks)

The first Electric Infrastructure Security (EIS) Summit took place in London on September 20, 2010, in the U.K. Parliament, Westminster Hall. As the first world summit on infrastructure security, EISS London founded a new international security framework designed to foster information sharing, discussion, coordination and cooperation in assessing and protecting national infrastructures against physical threats such as EMP and Severe Geomagnetic Storms.

The second EIS Summit will take place in the Capitol Building, Washington D.C. on April 11, 2011. To apply for registration for EISS Washington D.C., please email info@eissummit.com

NSWG Contact: Sanjit Singh, Sanjit.Singh@mail.house.gov or 5-4576 in Rep Franks' office

Question or comments regarding RSC National Security Working Group items can also be directed to Bruce F. Miller, bruce.miller@mail.house.gov