

*Christine O Gregoire, Governor, State of Washington
and
Mark A Emmert, President, University of Washington
despite warnings have permitted
Computing and Communications, University of Washington
to conduct an unlawful cyberwar on this
International Electronic Magazine
following publication of an article that exposed malfeasance.*

Denial-of-Service Attacks (DoS Bots)

Direct democracy has become extremely susceptible to irresponsible government officials who have access to substantial amounts of money and use it to control media and terms of debate. Deliberative democracy requires, and substantial empirical evidence shows, that the electorate frequently changes its mind about policy makers after an opportunity properly to reflect on the issues.¹

Mark A Emmert, President, University of Washington and Christine O Gregoire, Governor, State of Washington have known about unlawful denial-of-service attacks by their computing and communications staff for four and twelve years respectively then granted the hackers impunity through *laissez faire* policies. They have now permitted state employees to start a Cyberwar. [Anarchy]

Denial-of-service attacks affect all journalists as seen from last year's debacle in Estonia which set a dangerous precedent. Similar behavior now takes place globally, particularly in China and the United States. A cyberwar weapon, these attacks involve assault on electronic communication networks in retaliation for publishing unpopular opinion. [The New York Times - Estonia]

An increasing number of high-level officials in government and public institutions condone these illegal attacks upon freedom of expression. They give implied permission or impunity which allows the lowest level of Machiavellian behavior and disingenuousness conveniently disguised in the academe as "political science" and in commerce as "risk management". Properly called political expedience and coercion strategies, impunity allows cyber-censors to violate journalism and human rights protected by international laws. [Impunity]

Gregoire and Emmert received specific warnings that they must stop denial-of service attacks and address the issues (29 Jan 08). Instead, they have allowed a massive increase in coercion and harassment to reinforce their previous attempts to prevent publication of content that exposes criminal activity which they have condoned.

University of Washington employees, under the direction of Ronald A Johnson and Sandra S Moy, Computing & Communications (UW/C&C), with impunity granted by Mark A Emmert in collaboration with Carol S Niccolls, Special Counsel to the President, have vandalized this web site in order to destroy academic and journalism databases and computer systems that support them.

During the past two months they have transmitted denial-of-service bots which have caused actual and collateral damage in excess of \$150,000.00 to databases, systems, web pages, and subscriber networks. Evidently, they have again tried to coerce the author to cease publication or to cause him bankruptcy to a similar end. The cost of the damage rises daily as UW technicians continue (at this writing) to use their bots to prevent publication of subscriber newsletters and media releases by interfering with systems operation.

"Hackers either write bot programs themselves or reuse or modify existing code" wrote David Dittrich, an acknowledged expert on denial-of-service attacks until recently employed as a software engineer working for UW/C&C at an annualized taxpayer-funded salary of \$103,536.00/pa.

Dittrich published the following comments concurrent with UW/C&C implementation of identical denial-of-service attacks. Outrageously, he used taxpayer funds to publish "how to" essays (complete with coding algorithms) which will enable future cyber terrorists to launch attacks on unsuspecting computer users.

Some attackers have even installed bots on multiple machines to create a distributed system that can be used for complex attacks . . . such systems can launch distributed dictionary attacks to steal victims' passwords. . . . It seems like a logical progression that people have added programmable [attack] mechanisms to the bots to add functionality . . . advances in technologies such as wireless communications will increase the number of devices, systems, and network types that bots can take over and use as bases for attacks.

Computing and Communications (UW/C&C) has used all those tactics to try to destroy *Contra Cabal* and in so doing has destroyed equipment, operating systems, and databases.

Denial-of-Service (DoS) attackers, the most under-reported vandals in the industry, attempt to prevent legitimate users from accessing information or services. By targeting a computer and its network connection, the hacker can prevent users from accessing email, web sites, online banking accounts or other services that rely on the affected computer. By repeatedly sending large email messages to an account, an attacker can exceed byte quotas and prevent delivery of legitimate messages.

Bots take advantage of system software bugs which enable buffer overflows and various memory-management problems that allow malicious code to infect a system. They operate automatically as an agent for a hacker or an automatic program.

Hackers also "flood" web sites and email accounts with massive amounts of information in order to crash them. When a user accesses a particular web site by entering an URL in a browser, a

request transmits to the Internet Service Provider (ISP) server to view a page. The server can only process a certain number of requests at once. If an attacker overloads the server with requests, then it crashes the system.

Vandals (hackers) send bots to victims by a variety of means to infect vulnerable computers. Some bots wait for commands from the hacker who can manipulate them and the infected systems remotely. Most computer users have familiarity with viruses, worms, Trojan horses, and network intrusions on a regular basis and know how to protect themselves. However, virtually no protection exists against bot software.

Denial-of-service attackers can use either their own computers or machines that they have infected which then act as proxy servers making it difficult for security investigators to find the culprits.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even DNS root servers. One common method of attack involves saturating the target (victim) machine with external communications requests so that it cannot respond to legitimate traffic or responds so slowly which renders it effectively unavailable.

Denial-of-service attacks violate Interactive Advertising Bureau (IAB) Internet use policy. They also violate US and EU laws also laws of individual nations. Unfortunately, there are no effective ways to prevent victimization by a DoS attack. One can only install ant-virus software, firewall applications and other protective devices to reduce the risk that an attacker will use a single computer to attack other computers.

Conclusion

Voters can only reflect if they have uncensored information to discuss with fellow citizens and policy experts. After deliberation, they routinely alter their preferences in durable and unpredictable ways.

As governor of a state that claims democracy, Gregoire must: allow the electorate to decide the issues after web access and an opportunity to read all information relative to both sides of any particular issue; carry out her duty and responsibility to protect freedom of expression and the flow of information; stop condoning and granting impunity to censors and government-funded technologists who attempt to destroy journalists and the media; issue orders publicly to University of Washington to cease and desist the use of unlawful means and taxpayer resources to fund denial-of-service attacks and harassment of journalists; otherwise, she has an international cyberwar to contend with prior to her reelection attempt.

Governors of most US states hold qualified immunity dependent upon the scope of discretion and responsibilities of the office. This allows the executive branch to attract high-quality candidates for election to government service. Reasonable grounds, coupled with good-faith, afford a discretionary

basis for immunity from lawsuits for official acts performed by Christine O Gregoire, Governor, State of Washington.

US Supreme Court has determined that executive immunity bears the burden of justification based upon the nature of the act performed, not the identity of the actor who performed it. Political expedience coupled with bias defines as malfeasance and provides probable cause for lawsuits against governors who do not enforce constitutional guarantees.

In deciding probable cause for impeachment, a reasonable person must ask four questions that relate to any challenged act, omission, or decision:

1. Did the act involve a basic governmental policy, program, or objective?
2. Was it essential to the execution of that policy, program, or objective?
3. Did it involve agency policy evaluation, judgment, and expertise?
4. Did the agency possess constitutional, statutory, or lawful authority to ratify the decision?

If clear and unequivocal answers in the affirmative result, then the challenged act, omission, or decision can, with reasonable confidence, classify as a discretionary governmental process regardless of its lack of wisdom. If one or more of the questions call for, or suggest a negative answer, then an official inquiry must take place into the facts and circumstances.

Any inquiry must premise upon whether Gregoire, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjected, or caused to be subjected, a citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, which would make Gregoire liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.

Washington state electorate presumably consists of reasonable people who must decide whether Christine O Gregoire, Governor, formerly Attorney General, can answer all four questions affirmatively given the extensive, documented malfeasance described in *Contra Cabal*. [Anarchy]

Reprise of article published (18 Mar 08). Emmert and Gregoire received two prepublication notices (29 Jan 08 and 5 Feb 08) which they have both ignored.

Internet Censorship

Computer Hacking and Cracking

Mark A Emmert

President

University of Washington

Contra Cabal editor sent a prepublication notice to Mark A Emmert, President, University of Washington, and twenty other top administrators, to announce a new series:

The Ultimate Machiavelli

The notice gave them an opportunity to respond to alleged malfeasance prior to general release of the article to the public. The email message (5 Feb 08) contained this admonition:

This notice is sent as a courtesy to people mentioned. The articles remain "live" in that they are subject to continual update when new information surfaces. As works in progress, they will link to personal case studies as time or relevance permits.

An unlawful pattern or practice already exists among named University of Washington administrators and faculty members who have attempted to flood this web site, destroy databases, damage computer servers, or otherwise interfere with publication of *Contra Cabal*.

Any attempt to continue that practice, or indulge in prior restraint by other means, will immediately become subject to reports to Federal Bureau of Investigation. International and federal laws preclude electronic interference with dissemination of information. Contra Cabal uses secure servers and detection software to expose malfeasance - Mark Emmert, take notice and be warned!
[Full Text PDF PT-08-0205-1725]

Censored Releases

College of Education

College of Engineering

School of Nursing

Malfeasance - University of Washington

Department of Technical Communication, UW

Malfeasance - UW School of Nursing

Instead of responding to the issue, Emmert apparently tried to kill the messenger. He has allowed his technical staff to censor email by randomly deleting text from personal email messages and

crashing computers to try to prevent publication of content protected under First Amendment to US Constitution.

Although Emmert has received repeated warnings about this violation of federal law, UW computer technicians continue to sabotage Contra Cabal systems and web sites on a regular schedule. Federal Bureau of Investigation (FBI) will receive a report about these malicious acts.

Since Emmert became UW president almost four years ago, he has received a stream of reports of violations of federal law. Instead of heeding requests and warnings he repeatedly allowed UW computer technicians to sabotage computer systems and web sites. He has simulated the pattern or practice initiated by his predecessor Richard L McCormick in collusion with Ronald A Johnson and Carol S Niccolls his special counsel. Gregoire (as attorney general, governor and Niccolls's mentor) has for twelve years condoned multiple malfeasance by neglect to uphold the law.

Johnson, a university employee, has for more than twelve years instructed or allowed his technicians to: crack into computer systems; flood web sites; destroy academic databases; censor incoming and outgoing email; sabotage operating systems; deny access to paid accounts; coerce commercial internet providers to restrict service; and used taxpayer funds to cause damage to private computer systems and databases in excess of \$50,000.00.

[Computer Crackers - University of Washington]

Niccolls colluded with Johnson to destroy academic research databases, denied access to paid accounts, and has participated in multiple other frauds. A former assistant attorney general (AG) under Governor Christine O Gregoire (former Attorney General), Niccolls will eventually have to answer a Washington State Bar Association, Rules for Professional Conduct (WSBA) complaint in company with other AG and UW lawyers. They intercepted or diverted US mail and email addressed to UW regents and other top echelon administrators allegedly to keep them in ignorance of crimes committed by lower echelon employees.

[RPC Rule 8.4 Misconduct]

Emmert inherited both Johnson and Niccolls from McCormick and promoted Niccolls to Special Counsel to the President. Despite their malfeasance, Emmert has increased Johnson's salary from \$252,000.00/pa to \$321,684.00/pa, an increase of \$69,684.00 (27.65%/4), and increased Niccolls's salary from \$138,000.00/pa to \$190,560.00, an increase of \$52,560.00 (38.08%/4).

[Roll of Dishonor Case Studies]

Faculty members who receive comparatively meager remuneration, also students and parents who pay exorbitant tuition or fees, should remember these excesses when they consider reelection of a governor who has condoned criminal behavior by successive UW presidents.

[Nothing Succeeds Like Excess]

Nemesis.

1. Ethan J. Leib, Can Direct Democracy Be Made Deliberative? *Buffalo Law Review*.

© Copyright 2008 by Paul Trummel

All Rights Reserved: 17 Apr 08/17:36

Edition: #608-01-00/08-0421-0632

Feedback: Webspinner@ContraCabal.org