Survivability Issues and Challenges

James B. D. Joshi
University of Pittsburgh, USA

Suroop M. Chandran
University of Pittsburgh, USA

Aref Walid
Purdue University, USA

Arif Ghafoor
Purdue University, USA

INTRODUCTION

An electronic government (e-government) is essentially an amalgam of interconnected heterogeneous information systems belonging to both government agencies and public and private sectors with a goal of modernizing the government's highly fragmented service-centric information infrastructure by improving information flow and the decision-making process (Joshi, Aref, Ghafoor, & Spafford, 2001a). The e-government environment also embeds the nation's critical infrastructures, that are required for providing the nation's basic services to the citizens (PDD, 1998), such as energy, telecommunications, banking and finance, and transportation facilities. The intricate connectivity of systems and their increasing dependence on IT dramatically magnifies the consequences of damages resulting from even simple system faults/accidents and intrusions, as well as natural events (fire, earthquakes, etc.), also collectively called *disruptions* (Ellison et al., 1997). A key challenge for such an infrastructure is to ensure continuous service availability to prevent financial losses, loss of prestige, endangerment of citizens' lives, and disturbances in national socio-psychological structures adversely effecting governance and democracy (Ellison et al., 1997; Gibbs, 1994; Moore, Ellison, & Linger, 2001). While it is essential that the e-Government infrastructure is resilient to disruptions, an even bigger concern is the protection of critical infrastructure components within the e-government. In essence, the e-government infrastructure should have the capability *to provide services in a timely manner, irrespective of disruptions*, a capability known as *survivability*.

E-GOVERNMENT SYSTEMS SURVIVABILITY

The e-government survivability infrastructure should support both the intricate interdependence of government programs at different levels and between government and the private/public sectors, and address the need for continuity of its services in presence of disruptions. While such disruptions are inevitable in an e-government, key to its success lies on the effectiveness of mechanisms for detecting and responding intelligently to disruptions, which is a daunting challenge. Intelligent distributed capability is required to detect and counter both structured and unstructured disruptions that can be either in the form of intrusions or faults. Intrusions refer to the illegal access to a system by an intruder, whereas faults refer to the causes of physical failure of a system. Intrusions can be detected with the help of intrusion detection systems (IDS). IDSs report *anomalies* in behavior or recognize intrusion *signatures*. Faults can be detected but more importantly, methods for fault tolerance have to be implemented in the system. Fault tolerance is the ability of a system to withstand physical failure.

A survivability system needs to employ a combination of intrusion detection/prevention and fault tolerance methods. Separation between faults and intrusions, which have been studied separately, does not leverage the synergy existing between the two areas. This increases the overall cost of deploying measures against them, as well as the complexity of the overall system. Newly emerging coordinated, distributed intrusion detection techniques, coupled with data mining or stream mining tech-

Table 1. Threats and their intent (Alexander et al., 1999)

Threat level	Actor	Intent
National security threats	Information Warrior (Cyber-soldier)	Reduce decision making capability at the national level, National chaos and psychological terror
	National intelligence (Cyber-spy)	Information leakage for political, military and economic advantages
Shared threats (government & Private sector)	Cyber-terrorist	Visibility/publicity, chaos, political changes
	Industrial espionage	Competitive advantage
	Organized crime (Cyber-crime)	Revenge, retribution, monetary gain, institutional/political change
Local Threats (Hacktivism)	Institutional hackers	Monetary gain, thrill/challenge, publicity/prestige
	Recreational hacker	Thrill, challenge

niques show promise in improving the survivability capability of a large infrastructure like that of an e-Government system by facilitating real-time detection of and responding to disruptions.

Disruption Categories for E-Government Systems

Disruptions to e-government services can be divided into two categories—*cyber disruptions* and *critical infrastructure disruptions*. Cyber-disruptions include cyber-terrorism, like NIMDA and the Code Red worms, and information warfare. Potential "*info weapons*" that can be used to launch an attack on an e-government include computer viruses, logic bombs, worms, Trojan horses, etc. (Alexander & Swetnam, 1999; Denning, 2001; Garfinkel & Spafford, 1997). Various attacks on systems include denial of service attack, virtual sit-ins and blockades, rootkits, etc. (Denning, 2001). The attacks using these malicious tools range from simple hacktivism, which refers to active hacking activities with the intent to disrupt normal operations but not causing serious damage, to the more damaging *cyber-terrorism* and *information warfare* (Alexander et al., 1999; Denning, 2001), which have become growing concerns post 9/11 era. Information warfare refers to the large-scale malicious activities launched by independent individuals or attackers hired by terrorists or belonging to rival countries. Cyber-terrorism is a more dangerous form of cyber-disruptions that can cause severe damage to the nation's systems (Denning, 2000). Even a simple, hour-long coordinated hacking activity that affects the country's air traffic system, a critical infrastructure, can have very drastic consequences for government operations. In a few years, the cyber-threats to the country is expected to be worse than the physical threat (Alexander et al., 1999).

Critical infrastructure disruptions could be some malicious attack, accident, or disaster causing critical infrastructure malfunction, which becomes a national concern. Protection of critical infrastructure is an important issue, because any disruption in their functioning would cause nation-wide chaos, for instance, the North-East Blackout of 2003 in the United States and Canada—a power failure over the Northeastern regions of the United States and Canada in 2003 that caused many systems dependent on the electrical grids to fail disastrously. The damage was estimated at almost U.S. $5 billion (Anderson et al., 2003).

Table 1 shows various threat levels and the criminal intent behind them (Alexander et al., 1999). At the highest level, we see national security threats, which are essentially aimed at the nation's critical infrastructures. Threats common to both government and non-government agencies include cyber-terrorism and e-espionage. Finally, there are frequently occurring hacking incidents that can create huge losses within an e-government environment. An alarming issue is the lack of awareness and ability to identify cyber-threats. Newer spamming and phishing attacks make survivability function more difficulty to implement (GAO, 2005).

At present, there is no nationally coordinated defense and survivability capability to detect and counter strategic and well-coordinated act of cyber-terrorism against the nation and to ensure the continuity of e-government services under cyber-siege. The U.S. National Infrastructure Protection Center (NIPC) is a program started by the Clinton administration in 1998 with an intention to maintain public and private sector infrastructure from disruptions of any sort and perform vulnerability checks regularly as preventive measures. Other nations such as Canada (PSEPC) and New Zealand have also taken to emergency preparedness and critical infrastructure protection. The Critical Infrastructure Protection project focuses on the impediments to the security and protection of the assets and addresses *public-private cyber-security cooperation, industry-academia consortium, knowledge management long-term high-risk cyber-security research.*

AN ADAPTIVE E-GOVERNMENT INFRASTRUCTURE SURVIVABILITY FRAMEWORK AND ITS CHALLENGES

The key e-government survivability challenge is to synthesize a unified adaptive survivability framework (ASF)