Serious cyberattacks have been in the news quite a lot recently. Large organizations in the United States, including Lockheed, Google, Citigroup and the International Monetary Fund, have all reported successful attempts perpetrated against them. Particularly discomforting was the attack on EMC Corp.’s RSA division, which was, in effect, a meta-attack in that what the hackers were reported to have stolen was security information related to the access control tokens used by millions of individuals around the world.

Beyond Hacking
By all indications, these are not examples of hacking, at least not as the term has been used for many years. The reported attacks were not attempted by mischievous teenagers seeking to create random damage just to show that they could do it. These were deliberate attacks with intent to cause some sort of harm. In some cases the motivation seems to have been monetary. In others, groups or individuals that are somehow aggrieved seem to have been seeking to exact revenge. Still others are said to be geopolitical in nature. There have even been incidents in which open military conflict was said to have included cyberwarfare.

Allegations have also been made that cyberattacks were used as instruments of policy by one nation against another. The nation of Estonia was victimized so greatly that it found itself losing “the first war in cyberspace,” described in The New York Times as “close to shutting down the country’s digital infrastructure, clogging the web sites of the president, the prime minister, Parliament and other government agencies, staggering Estonia’s biggest bank and overwhelming the sites of several daily newspapers.” The so-called Stuxnet worm was evidently aimed at Iran’s nuclear program; “computer security specialists who have examined it were almost certain it had been created by a government and is a prime example of clandestine digital warfare.”

Not Reported
In reading about these numerous examples of cyberwarfare in our times, I was struck by something I did not read. In many cases social networking services have been instrumental in what has become known as the Arab Spring, a wave of rebellions and outright revolutions across Northern Africa and the Mideast. For example, a Google executive in Egypt, Wael Ghonim, “was a quiet force behind the YouTube and Facebook campaigns that galvanized Egyptian protesters in January 2011”; when he was arrested during the uprising, “hundreds of Egyptians took to Twitter and the Internet, calling on him to become one of their new leaders.” It is, therefore, fair to say that many of those involved in the Egyptian events and those in other countries were computer-savvy. But, there have been no reports, of which I am aware, of cyberattacks on ruling governments (or rebels, for that matter). This startling omission leads to a train of possible conclusions that I find very disturbing, namely:

- Maybe governments were attacked by rebels but did not report it. If this did happen, I can understand why the governments in question would not want to publicize the fact that their systems were undermined by members of their civilian populations. But, I cannot understand why the rebels, especially those who have overthrown their rulers, would keep their exploits secret.
- Cyberattacks are not easy to execute. If people were well versed in the use of computer systems have not been perpetrating such attacks as a component of their revolutionary activities, it probably is not as simple to pull off as one would believe reading the works of Steig Larsson. These people in the Arab countries had more than enough incentive to undermine the systems of their countries’ militaries and police forces. They had the motivation and opportunity, but apparently not the technical or intellectual means.
Governments do have the skill to conduct cyberattacks. Perhaps it would be more accurate to say that, as of now, only governments or organizations sponsored by governments have those skills. Therefore, if governments are actively developing these skills, they intend them to be a supplement to—or possibly a replacement for—their arsenals in full-scale shooting wars in the future.

Cyberattacks are not the moral equivalent of war; they are war. This is not simply my opinion. General Kevin P. Chilton, the head of the US Strategic Command, told reporters that in the event of a cyberattack, “the law of armed conflict will apply,” and warned that “I don’t think you take anything off the table in considering a response. Why would we constrain ourselves?”

Cyberattacks are a real, clear and present danger to many corporations and government agencies. If it has happened, it can happen. The fact that there have been so many reported attacks on databases and web sites is indicative of the reality of the threat. The motivations of vandals are different from those of criminals, and those of warriors are very different from those of criminals. If it is governments or government-backed groups that are behind the wave of recently experienced attacks, the perpetrators are very motivated indeed, and may have the resources necessary to target the largest institutions.

Targeted organizations are unprepared for the dangerous train that is approaching. The organizations that have publicly admitted to having been attacked are some of the largest and most sophisticated in the US, if not the world. They are aware of the sensitivity and criticality of their information resources and have taken extensive measures to protect them. And yet, their information resources were successfully penetrated. The type of hacking experienced in the past is substantively different from what these organizations may be facing today; this train is cannonballing down the track.

Security professionals are at risk. On a personal level, if I follow this chain of conclusions to its logical end, I realize that those of us who deal with the security and control of information (and are represented among ISACA’s membership) could be the targets of cyberattacks. Just as RSA was attacked to obtain the metadata of security, so the information security professionals of the world have a huge amount of sensitive information in their file drawers, their hard drives and their heads. It might be possible to piece together bits of information that would open their employers’ databases to malicious misuse by those who have the wherewithal to make the most of it.

I said that the train of conclusions in this article was disturbing. It is particularly disturbing to realize that the last stop on that train is me and many people I know.

ENDNOTES
1 This was written in June 2011. I’m certain there will be many more such reports by the time this is read.
2 Drew, Christopher; “Stolen Data Is Tracked to Hacking at Lockheed,” The New York Times (NYT), 2 June 2011. The New York Times is often referred to as the US paper of record. Accordingly, where there is no primary source, I quote the Times. For this reason, there is a bit of an American perspective to the incidents cited, but it is also clear that this is not solely an American problem.
3 Markoff, John; David Barboza; “F.B.I. to Investigate Gmail Attacks Said to Come From China,” NYT, 2 June 2011
5 Sanger, David E.; John Markoff; “I.M.F. Reports Cyberattack Led to ‘Very Major Breach’,” NYT, 11 June 2011
7 Markoff, John; “Georgia Takes a Beating in the Cyberwar With Russia,” NYT, 11 August 2008
8 Landler, Mark; John Markoff; “Digital Fears Emerge After Data Siege in Estonia,” NYT, 9 May 2007
9 Markoff, John; “A Silent Attack, but Not a Subtle One,” NYT, 26 September 2010
10 “Wael Ghonim,” Times Topics, NYT, 8 February 2011
11 And, if you have not read his works, I am certainly not going to give away anything here.
12 Sanger, David; Elisabeth Bumiller; “Pentagon to Consider Cyberattacks Acts of War,” NYT, 31 May 2011

AUTHOR’S NOTE
As ever, I invite readers to send me e-mails at stross@riskmastersinc.com with any comments or questions on this column. There is also a comments tab on the Journal article pages of the ISACA web site (www.isaca.org/journal) where readers may enter comments. I promise to check this area regularly and respond to both sources of dialog with Journal readers.