ATTACKS on U.S. computer systems happen every day. Officials from the National Security Administration report that the computer systems that control the United States nuclear arsenal alone withstand up to 10 million attacks a day.

The cybersecurity industry that aims to protect the U.S. from these attacks will grow to $207 billion this year, according to an April 2013 report by industry research firm IBISWorld. But striking a balance between the openness and speed of the Internet—qualities that make it so powerful and useful—with the firewalls and protocols necessary to ensure a stout defense is the key dilemma faced by experts in the war on cyberterrorists.

Law School Professor Michael Greenberger, director of the University of Maryland Center for Health and Homeland Security, reinforces that it’s almost impossible to offer an ironclad defense against the significant threat posed by a “strategic and surgical” cyberterrorism attack on electrical grids or the banking system.

“It’s not hype,” observes Greenberger. “Anyone who knows anything about terrorism will tell you that the most likely catastrophic terrorist attack is a cyberattack.”

In many respects, the law itself hasn’t caught up with the speed of changes to privacy and commerce wrought by the digital age.

First, there is no concrete, universally agreed upon definition, informally or legally, as to what defines an act of cyberterrorism. Academia, the dictionary, and even the FBI all have slightly different viewpoints.

By the most rigorous standards, a true act of cyberterrorism has never been used against the United States, despite an ongoing cyberwar propagated by nations and
non-state agents alike. Most definitions call for acts to be politically based and catastrophically destructive.

This definition, however, does not negate the reality that, despite society’s inability to name them, assaults occur daily on privacy, commerce, government infrastructure, corporations, media organizations, and universities, to name a few. Nor does it take into consideration physical acts of terror that are planned and organized online through social media.

Technology has the ability to make gray what was once the black letter of the law.

The USA Patriot Act of 2001 passed in response to 9/11 has been repeatedly amended to contain penalties for cyberterrorism, as well as more rigorous definitions of what entails an act of cyberterrorism.

But precedent-setting case law is still being decided as the threats become even more complicated.

Developing a pool of leaders with expertise in the field is increasingly necessary, Greenberger notes. Not only must state and federal legislators navigate tensions between civil libertarians and law enforcement as they write new laws, but regulators and law enforcement officials must also cope with the reluctance of businesses to shoulder the costs of preventing cyberattacks and other Internet crimes.

Efforts to train a new generation of lawyers (many of whom may end up in government) to cope with the seismic shifts of our digital age are enhanced by the Center for Health and Homeland Security and a UM Carey Law course on Law and Policy of Cybersecurity.

“Most places might teach [cybersecurity] as a subtopic in a broader course, but for the second year we are teaching a [stand-alone] course on this subject,” says Greenberger, who designed the course.

Two analysts affiliated with the Center—Ellen Cornelius ’05 and Markus Rauschecker ’06—are now teaching the course, which was developed in response to demand from Center clients. Rauschecker observes that the field of cybersecurity is moving so fast that the beginning of each class session is devoted not to case law or theory but to an analysis of current events.
“Things are changing even as we teach the course,” he says. “We’ve had to be flexible in that regard, but it’s made the course even more exciting for the students.”

The seminar is also giving UM Carey Law students a chance “to be involved in a field when it’s really at the beginning and help shape where it goes,” says Rauschecker. And the Center’s relationships with key players in the cybersecurity sector—who often come to speak to the class—allow students to test the ideas that they’ve formulated against the expertise of those actually involved in protecting against attacks.

“The students see that it isn’t just a theory,” Rauschecker says. “They see how these things are actively happening in the real world.”

Greenberger fears that a catastrophic cyber assault on our nation’s vital infrastructure may see a repeat of government’s post-9/11 scramble to play catch-up with a new wave of terrorists, further transforming the landscape of personal freedoms and commerce.

“We can’t get much-needed cyber legislation through Congress,” he says. “And business doesn’t want to be told what to do. If we have a major crisis, I’m not saying civil liberties will be disregarded, but those concerns will not be predominant and we will get cyber legislation. Congress will ultimately be forced to do this.”

ENHANCING CYBERSECURITY IN MARYLAND

CYBERSECURITY reform is a primary focus in the state of Maryland, which in 2010 and 2011 ranked third for per capita identity fraud complaints, and ninth for per capita identity theft complaints. Authorized by the Maryland General Assembly in 2011, the Maryland Commission on Cybersecurity Innovation and Excellence is charged with conducting an overview of federal and state cybersecurity laws and policies, considering Maryland’s role in promoting cyber innovation, and recommending a comprehensive framework and strategic plan for cybersecurity, including recovery from cyberattacks.

Center for Health and Homeland Security law and policy analysts Avery Blank ’11 and Peter Suh ’09 worked with the Commission, of which Professor Michael Greenberger is an appointed member, on legislation that was introduced in the 2013 Session and testified on behalf of the Commission before various Maryland Senate and House Committees.

“The Commission is dedicated to enhancing cybersecurity protections for the citizens of Maryland,” said Suh in a recent email. “It was an honor to explain to our State Senators and Delegates how the Commission’s bills would enhance cybersecurity protections for Maryland residents.”

As a result of the Commission’s work, the Maryland General Assembly recently passed legislation that requires certain state government units, such as public institutions of higher education and local agencies, to notify individuals of a breach of personal information. The Commission will continue its work through 2013 and 2014 and will present a final report of recommendations and findings to the Governor and General Assembly by September 1, 2014.