David is like a man possessed. For days on end, he sits in his room in front of a black screen with glowing green script. Over and over, he types columns of cryptic letters and numbers into his computer. Actually, David Lightman is a high school student. At home, however, he turns into a hacker. The irreverent whiz kid hacks into his school’s computer database and manipulates the grades of his friend Jennifer. He out-

Broderick his first Oscar nomination in 1983 – and gave the rest of the world its first uncomfortable inkling that an out-of-control computer could do enormous damage via the global data network. At that time, only a few experts were familiar with computing. Laypeople viewed hackers with a peculiar sense of admiration, seeing them as an exotic breed that navigates its way on invisible paths through a strangely abstract cosmos. In 1983, the virtual world was making its first tentative forays into kids’ rooms and living rooms with Atari and Commodore 64.

Today, nearly 25 years later, the world looks very different. It is no longer just businesses and government agencies that are digitally linked. A dense data network has long since encircled the globe, linking billions of people worldwide. In Germany, logging on to the Internet is a matter of course for 75 percent of 18- to 34-year-olds. Information speeds around the globe in milliseconds – billions of e-mails, documents and images daily. X-ray images whiz back and forth between continents, from specialist to specialist. Engineers even service power plants remotely via data cables.

With a simple key combination, anyone can bring the world’s knowledge into his or her home. In doing so, however, the user may unknowingly open the door to unwelcome guests. Alongside billions of law-abiding Internet users, there are thousands with malicious intentions. The dark side of the Internet now even has a name: cybercrime. The perpetrators are hooded terrorists who brandish their weapons in Internet videos and call for religious war, recruiting new fighters with their militaristic websites. Or swindlers who send trojans to snatch PIN numbers for online accounts. Or criminals who distribute photos of abused and tormented children in secret online marketplaces. The hackers of the early 1980s seem almost harmless in comparison.

**Construction Manuals for Bombs**

Today, cyberspace offers room for the entire spectrum of transnational criminal activity. And the law is not prepared for this. It reaches its limits particularly when the offenses become complex, when agencies are tracking organized crime and white-collar criminals around the entire globe, or when it has to untangle terrorist networks. Organized criminals and terrorists use encryption methods to communicate via the Internet. Terrorists publish construction manuals for bombs. They plan attacks through the data network and use search engines and Google Earth to scout potential targets.

Tracking down criminals in the anonymous, ephemeral and super-fast Internet is difficult enough, but prosecuting and convicting them is even harder. The main problem is with criminal law: the Internet is global, while criminal law is essentially limited to its respective national territory. In the case of traditional criminal activity, the perpetrator is usually physically present at the
crime scene and is subject to trial by a local court. In the case of Internet crime, however, there can be 10,000 kilometers between the criminal and the scene of the crime. Many court proceedings have demonstrated the impotence of law enforcement authorities in such cases.

Ulrich Sieber, one of the two directors at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, knows the limits of the law, and he knows of the criminal futures taking place on the world stage. He specializes in cross-border crime – organized crime, international terrorism, white-collar crime and cybercrime. With his colleagues in the Department of Criminal Law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing criminal law, the jurist analyzes the schemes cooked up by the criminals and to what extent existing...
has often failed due to the fact that lawmakers in many countries continue to think in terms of traditional sovereignty. The Organization for Economic Cooperation and Development (OECD), for example, is not allowed to impose rules and regulations on any of its member states. Instead, it simply publishes the names of countries that fail to implement recommended reforms, a technique known as “naming and shaming”. This method of applying pressure has often been successful. In many cases, it has led to the subsequent amendment of national laws.

In the meantime, many countries have begun harmonizing various aspects of their criminal laws on cybercrime. The most important consensus worldwide is likely the Council of Europe’s Convention on Cybercrime, which has been ratified by a number of countries, including Canada and the US. The Convention prescribes, for example, that the punishment of certain offenses uniformly, such as accessing data without authorization, deleting data without authorization and distributing child pornography. Furthermore, participating countries want to standardize Internet investigation measures. And the Convention on Cybercrime demands one more thing of its member states: the establishment of national contact centers that are available on a twenty-four-hour, seven-day-a-week basis.

Covered Tracks in Cyberspace

Hacker attacks wander through many computers from one continent to another. In this way, attackers can follow their tracks. This makes it difficult for investigators to trace the route back to the source because connection data is seldom stored for very long. Since hacker attacks touch the territory of multiple countries, tracing back the perpetrators has, to date, been particularly troublesome. Thanks to the national contact centers, the affected countries can now quickly and unbureaucratically coordinate searches and international investigations. Thus, the fight against cybercrime is proving to be a role model for cooperation in international criminal law. The models and solutions used here are likely to be transferred to other areas.

The current risks lead to fundamental changes in criminal laws because, very often, traditional deterrents fail: terrorism is not afraid of punishment. It is hoped that preventive measures can forestall suicide attacks. The models used here are likely to be transferred to other areas.

The Council of Europe recently commissioned the institute in Freiburg to analyze the Convention on Cybercrime and other international conventions. The researchers were asked to evaluate the currency of international regulations pertaining to cyberterrorism. Sieber concludes that there is a lot to be done, for security law is designed to discover and prevent crimes while they are still in the planning stage.

The group working with Ulrich Sieber wants to find out how the new security law affects the entire legal system, as well as the criminal law – not only with a view to cybercrime. "The Internet clearly shows how important this is. Current examples are the online search, which Germany’s Federal Court of Justice has just declared illegal – in no small part because of an article by Sieber: in a conventional search, following a technical approach, search results are only completely and, quite openly.

Warning against Terror Hysteresis

Online searches for ephemeral digital information are a disproportionately more severe invasion of the privacy of persons who may have years worth of personal data stored on their computers, such as tax returns, insurance statements and perhaps even personal journal entries. They are not even aware of the government’s hack attack. A similar situation applies to dragnet searches for wanted persons and new central databases to which prosecutors, secret services and numerous other agencies have shared access.

There is no doubt: the new risks and the technical changes of the information society require new concepts and regulations in criminal law as well as new alternative approaches. But the researchers in Freiburg warn that terrorism hysteria may lead to the unnecessary curtailing of civil rights – much like the current US administration’s war on terror. There, suspects can be held in custody for a long time without any proof of a specific crime. Citizens are wiretapped and monitored without a court order – purely as a preventative measure.

According to Ulrich Sieber, the new challenges should not only stimulate creativity with regard to new intervention and monitoring measures – it is just as important to develop new mechanisms for protecting civil rights. The Max Planck researchers are doing that, too. “Our major focus is on basic research,” says Sieber. However, he and his colleagues also incorporate concrete, day-to-day problems of criminal law in their work. The Internet is of particular interest to Sieber. “It is a gigantic source of knowledge and a valuable good,” he says. One of his visions is to make the Internet into a globally protected legal interest, safeguarded by a global convention, just like has already been done for the high seas, Antarctica and outer space.

On the way to court: Ulrich Sieber (center), head of CompuServe Germany, Felix Simon (right), and attorney Wolfgang Diegfelder.

The new dangers of complex crime, however, call instead for a security law that focuses on prevention. Using novel monitoring methods, this security law is designed to discover and prevent crimes while they are still in the planning stage.

The group working with Ulrich Sieber wants to find out how the new security law affects the entire legal system, as well as the criminal law – not only with a view to cybercrime. The Internet clearly shows how important this is. Current examples are the online search, which Germany’s Federal Court of Justice has just declared illegal – in no small part because of an article by Sieber: in a conventional search, following a technical approach, search results are only completely and, quite openly.

Warning against Terror Hysteresis

Online searches for ephemeral digital information are a disproportionately more severe invasion of the privacy of persons who may have years worth of personal data stored on their computers, such as tax returns, insurance statements and perhaps even personal journal entries. They are not even aware of the government’s hack attack. A similar situation applies to dragnet searches for wanted persons and new central databases to which prosecutors, secret services and numerous other agencies have shared access.

There is no doubt: the new risks and the technical changes of the information society require new concepts and regulations in criminal law as well as new alternative approaches. But the researchers in Freiburg warn that terrorism hysteria may lead to the unnecessary curtailing of civil rights – much like the current US administration’s war on terror. There, suspects can be held in custody for a long time without any proof of a specific crime. Citizens are wiretapped and monitored without a court order – purely as a preventive measure.

According to Ulrich Sieber, the new challenges should not only stimulate creativity with regard to new intervention and monitoring measures – it is just as important to develop new mechanisms for protecting civil rights. The Max Planck researchers are doing that, too. “Our major focus is on basic research,” says Sieber. However, he and his colleagues also incorporate concrete, day-to-day problems of criminal law in their work. The Internet is of particular interest to Sieber. “It is a gigantic source of knowledge and a valuable good,” he says. One of his visions is to make the Internet into a globally protected legal interest, safeguarded by a global convention, just like has already been done for the high seas, Antarctica and outer space.

The new dangers of complex crime, however, call instead for a security law that focuses on prevention. Using novel monitoring methods, this security law is designed to discover and prevent crimes while they are still in the planning stage.

The group working with Ulrich Sieber wants to find out how the new security law affects the entire legal system, as well as the criminal law – not only with a view to cybercrime. The Internet clearly shows how important this is. Current examples are the online search, which Germany’s Federal Court of Justice has just declared illegal – in no small part because of an article by Sieber: in a conventional search, following a technical approach, search results are only completely and, quite openly.

Warning against Terror Hysteresis

Online searches for ephemeral digital information are a disproportionately more severe invasion of the privacy of persons who may have years worth of personal data stored on their computers, such as tax returns, insurance statements and perhaps even personal journal entries. They are not even aware of the government’s hack attack. A similar situation applies to dragnet searches for wanted persons and new central databases to which prosecutors, secret services and numerous other agencies have shared access.

There is no doubt: the new risks and the technical changes of the information society require new concepts and regulations in criminal law as well as new alternative approaches. But the researchers in Freiburg warn that terrorism hysteria may lead to the unnecessary curtailing of civil rights – much like the current US administration’s war on terror. There, suspects can be held in custody for a long time without any proof of a specific crime. Citizens are wiretapped and monitored without a court order – purely as a preventive measure.

According to Ulrich Sieber, the new challenges should not only stimulate creativity with regard to new intervention and monitoring measures – it is just as important to develop new mechanisms for protecting civil rights. The Max Planck researchers are doing that, too. “Our major focus is on basic research,” says Sieber. However, he and his colleagues also incorporate concrete, day-to-day problems of criminal law in their work. The Internet is of particular interest to Sieber. “It is a gigantic source of knowledge and a valuable good,” he says. One of his visions is to make the Internet into a globally protected legal interest, safeguarded by a global convention, just like has already been done for the high seas, Antarctica and outer space.

The new dangers of complex crime, however, call instead for a security law that focuses on prevention. Using novel monitoring methods, this security law is designed to discover and prevent crimes while they are still in the planning stage.

The group working with Ulrich Sieber wants to find out how the new security law affects the entire legal system, as well as the criminal law – not only with a view to cybercrime. The Internet clearly shows how important this is. Current examples are the online search, which Germany’s Federal Court of Justice has just declared illegal – in no small part because of an article by Sieber: in a conventional search, following a technical approach, search results are only completely and, quite openly.

Warning against Terror Hysteresis

Online searches for ephemeral digital information are a disproportionately more severe invasion of the privacy of persons who may have years worth of personal data stored on their computers, such as tax returns, insurance statements and perhaps even personal journal entries. They are not even aware of the government’s hack attack. A similar situation applies to dragnet searches for wanted persons and new central databases to which prosecutors, secret services and numerous other agencies have shared access.

There is no doubt: the new risks and the technical changes of the information society require new concepts and regulations in criminal law as well as new alternative approaches. But the researchers in Freiburg warn that terrorism hysteria may lead to the unnecessary curtailing of civil rights – much like the current US administration’s war on terror. There, suspects can be held in custody for a long time without any proof of a specific crime. Citizens are wiretapped and monitored without a court order – purely as a preventive measure.

According to Ulrich Sieber, the new challenges should not only stimulate creativity with regard to new intervention and monitoring measures – it is just as important to develop new mechanisms for protecting civil rights. The Max Planck researchers are doing that, too. “Our major focus is on basic research,” says Sieber. However, he and his colleagues also incorporate concrete, day-to-day problems of criminal law in their work. The Internet is of particular interest to Sieber. “It is a gigantic source of knowledge and a valuable good,” he says. One of his visions is to make the Internet into a globally protected legal interest, safeguarded by a global convention, just like has already been done for the high seas, Antarctica and outer space.