Детлеф Древс
Генеральный директор компании «Фидус Крипт» (ФРГ) – Участника «Интерспутника»

УГРОЗЫ СУВЕРЕНИТЕТУ И НЕФОРМАЛЬНОМУ САМООПРЕДЕЛЕНИЮ В XXI В.

Мы живет в то время, когда информацию называют «нефтью XXI века». Те, кто владеет каналами передачи информации и, тем самым, имеет беспрепятственный доступ к информации, контролирует весь мир и владеет им. Информация может дестабилизировать государства, манипулировать фондовыми биржами, подрывать или разрушать техническую инфраструктуру. Цифровая информация пронизывает все сферы жизни современного общества вплоть до самых интимных сторон человеческого бытия. В век искусственного интеллекта и квантовых компьютеров практически не существует пределов для хранения и анализа информации. Этот процесс сопровождается растущей концентрацией сбора информации в руках небольшого числа мультинациональных сверхкорпораций. Правительства поддерживают такой ход вещей, финансируя долгосрочные соглашения о сотрудничестве, принимая соответствующие законы и пользуясь результатами сбора информации.

В качестве примеров можно упомянуть «облачный» бизнес компаний Amazon и Google, а также аналитическую систему Alladin фирмы Blackstone. Те же самые частные корпорации, действуя при поддержке государств и частично обходя международные правила, развертывают глобальные системы связи, которые нейтрализуют суверенитет национальных государств в сфере связи.

Симбиоз государств и экономики при получении информации будет углубляться и, на мой взгляд, на первое место здесь уже вышла экономика.

В этом процессе используется аппаратное и программное обеспечение, которое крайне уязвимо (возможно, намеренно) с точки зрения безопасности. Пробелы уже обнаружены в процессорах и операционных системах. Естественно, уязвимостью пользуются криминальные «эксперты» для взлома информационных систем. Это касается всех сфер жизни цивилизованного общества. Проблемы наблюдаются в управлении процессами промышленного производства, энергоснабжении, компьютерных сетях, смартфонах, телевизорах и холодильниках.

Традиционные способы и средства шпионажа не утратили свое значение при атаках на важные государственные и экономические цели и постоянно совершенствуются. Они применяются избранно и целенаправленно и по-прежнему опасны для сверхсекретной информации.

Detlef Drews
CEO of FidusCrypt – USG GmbH – Intersputnik Signatory

ENDANGERING SOVEREIGNTY AND INFORMAL SELF-DETERMINATION IN THE 21ST CENTURY

We live in a time when information is called the oil of the 21st century. Those who master the information channels and thus have unhindered access to the information, control and control the world. Information can destabilize states, manipulate stock exchanges and the economy, and disrupt or destroy technical infrastructures. Digital information permeates all areas of life in modern society, right down to the most intimate areas of human beings. In the age of artificial intelligence and quantum computers, there are almost no limits to the storage and evaluation of information. This process is accompanied by an increasing concentration of the information-gathering process in the hands of fewer multinational dominant corporations. Governments support this development by financing long-term cooperation agreements, supporting legislation and participating in the results of information gathering.

As examples of this process, cloud business from Amazon and Google can be mentioned here, but also the analysis system of Blackstone called Aladdin. It is also the same private corporations that, with state support, partly bypassing international regulations, are installing global communications networks that neutralise the sovereignty of nation states in telecommunications.

This process of the symbiosis of the state and the economy in the acquisition of information will continue to intensify, and in my view the economy has already taken the lead here.

This development is accompanied by hardware and software that has significant (probably intentional) security vulnerabilities. These gaps have already been proven in the processors and their operating systems. These vulnerabilities, of course, also remain not closed to criminal experts from the hacking scene and are targeted by them. No area of civilised societies is excluded. The problems range from process control in industry, to power supply systems, computer networks, to smartphones, televisions and refrigerators.

Traditional espionage methods and means have lost none of their importance in attacks on important state and economic targets and are constantly being refined. They are used in a targeted and selective manner and remain a danger for top-secret information.

Due the digital revolution in industry and the progressive digitalization of the public and private space using the Internet or the networks/services of multinational corporations, this development will continue

Благодаря цифровой революции в промышленности и продолжающейся цифровизации общественного и личного пространства с использованием Интернета и сетей/услуг мультинациональных корпораций этот процесс будет в ближайшие годы ускоряться и сделает государства, организации, компании и частных лиц прозрачными как стекло. Доступ к информации станет для владельцев сетей связи и «облачных»/аналитических центров прямым и оперативным в реальном масштабе времени.

Уже сегодня отмечаются следующие потенциальные угрозы:
1. Шпионаж во всех областях электросвязи с хранением полного объема данных, а также прямой доступ к конфиденциальной государственной и экономической информации, профилям частных лиц, их передвижениям, контактам, предпочтениям и т.д. Это касается как государственных деятелей, так и любого менеджера или продавца в магазине.
2. Целенаправленные диверсии на объектах инфраструктуры с использованием каналов связи или стандартных систем управления технологическими процессами.
3. Возможность целенаправленного манипулирования данными во время передачи. Это относится к изменению контента, а также задержкам или помехам передачи информации. Наполнение социальных сетей фальшивыми новостями может дестабилизировать политические системы и приводить к беспорядкам и мятежам, как уже неоднократно случалось.
4. Автоматическое обнаружение военнослужащих и сотрудников служб безопасности на особо охраняемых объектах, а также их контактов за счет изучения профилей перемещения.
5. Преднамеренное частичное или полное отключение сетей связи.
6. Хакерские атаки в интересах террористов и преступников за счет использования уже встроенных изготовителем уязвимых мест.

Эти шесть пунктов – всего лишь малая часть. При желании перечень можно легко продолжить.

Учитывая все эти процессы и угрозы, для ключевых объектов инфраструктуры и информации можно сделать следующие выводы:

1. Создание резервируемых государственных сетей связи с безусловным отсоединением от сети Интернет и разветвленных сетей мультинациональных корпораций. Для этого существуют прямые связи через спутники Земли и собственные наземные каналы с ограниченным числом узлов связи. Такие сети должны иметься в распоряжении крупнейших компаний и на ключевых объектах инфраструктуры.
2. Предоставление не только всех современных средств голосовой связи, передачи данных, видео, управления процессами, но и использование тематических чатов и приложений социальных сетей в рамках сети с шифрованием и через собственные серверы.
3. Разработка и применение собственных онлайновых систем шифрования (аппаратуры и программного обеспечения) с собственными алгоритмами шифрования. Отказ от коммерческих систем шифрования со стандартными криптоалгоритмами (например, AES256). Шифроваться должна вся информация во время передачи «от точки к точке» с использованием различных постоянно меняющихся алгоритмов и ключей. В век квантовых компьютеров системы шифрования должны быть полностью цифровыми, но параллельно использовать аналоговые способы шифрования.
4. Создание эффективной государственной организации для эксплуатации, обеспечения безопасности и управления сетями связи, группами серверов и системами/средствами шифрования.
5. Постоянное внимание секретоносителей в политике и бизнесе к осторожному применению современных методов и услуг.

Учитывая структуру спутниковых каналов, этот вид связи лучше всего подходит для организации безопасных сетей. Высокая доступность спутниковых каналов и возможность их гибкого резервирования играет особую роль. Для взломщика просушивание спутниковых линий крайне затратно технически и должно осуществляться непосредственно с эфира. В то же время, применение сложных систем онлайнового шифрования делает полученные данные бесполезными для взломщика. Становится невозможным маршрутизировать и отображать данные, например, в сети Интернет или в сетях мультинациональных корпораций, преднамеренно нарушать связь или вызывать бои в предоставлении индивидуальных услуг.

faster and faster in the coming years and lead to glass states, organizations, companies and individuals. Access to information for the deer owners of telecommunications networks and cloud/analysis centers will be possible directly and in real time.

The following potential hazards are already to be observed today:
1. Espionage in all areas of telecommunications with storage of all communication data, as well as direct access to sensitive state and economic data, person profiles, movement profiles, contacts, preferences, etc. This is regardless of whether an important statesman, manger or seller in a supermarket.
2. Targeted sabotage of technical infrastructure of states and industry via communication channels of standardized process control systems.
3. Possibilities of targeted manipulation of communication data during transmission. This concerns the modification of the content, as well as the delay or prevention of the transmission of information. By targeting social media with fake news, political systems can be destabilized, riots and unrest can be instigated, as has often happened.
4. Automatic detection of military and security personnel in specially protected objects, as well as their contacts via movement profiles.
5. Targeted switching off, of parts or entire telecommunications networks.
6. Attacks by hackers for criminal and terrorist activities by exploiting already manufacturer-invendor «implemented» vulnerabilities.

These 6 points are only a small selection and can be expanded as desired.

Taking these developments and hazards into account, the following key derivatives for key infrastructures and information can be made:
1. Creation of redundant state communications networks with strict decoupling from the Internet and widely branched communications networks multinational telecommunications corporations to. This is where direct satellite connections and our own terrestrial connections with few telecommunications nodes are available. This network will also be available to important companies and key infrastructures.
2. Providing all modern means of communication voice, data, video, process controls, but also chat rooms and applications of today's usual social media, within the independent encrypted network via own server centers.
3. Development and use of own online encryption systems (hardware and software) with own crypto algorithms. Do not use commercially available encryption systems with standardized crypto algorithms (e.g. AES256). Here, all information's during transmission end-to-end with different changing algorithms and key means must be encrypted. In the age of quantum computers, encryption systems should not be pure digital systems, but should also have analog encryption methods.
4. Creation of an effective governmental organization for the operation, security and control of communication networks, server centers and the encryption system e/-medium.
5. Constant awareness of holders of confidential information in politics and business on the careful use of modern means and services.

Due the structure of satellite connections, these are particularly suitable for the creation of secure communication networks. The high availability of satellite connections and the possibility of creating flexible redundancy plays a special role here. An interception of satellites by an attacker is technically very important and must be ensured off-air. However, the resulting data is worthless to the attacker through the use of complex online encryption systems. This means that it is not possible to conveniently route and mirror the data, such as on the Internet or the networks of multinational corporations, including a targeted disruption of communications or individual services.