Cybersecurity Law
Liability

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

Article 12 "Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
(a) the provider does not modify the information;
(b) the provider complies with conditions on access to the information;
(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Tallinn Manual 2.0

Rule 19 – Circumstances precluding wrongfulness of cyber operations
The wrongfulness of an act involving cyber operations is precluded in the case of:
(a) consent;
(b) self-defence;
(c) countermeasures;
(d) necessity;
(e) force majeure; or
(f) distress.

1. This Rule is based on the grounds set forth in Part One, Chapter V, of the Articles on State Responsibility. Should one of the enumerated circumstances exist, the action or omission in question will not be 'wrongful' and, therefore, the State engaging in the, or omitting required, conduct will not bear responsibility for what would otherwise be a wrongful breach of an obligation owed to the injured State. As will be discussed, the circumstances merely excuse nonperformance of the obligation while the condition exists; they do not extinguish the obligation altogether.

Dagstuhl Taxonomy:

1. Hacking into systems to identify the attacker
Attackers are using several techniques to hide their identification. One way is to hide themselves behind proxy chains provided by different hosting providers or compromised computer systems and located in different countries. In order to identify the attacker, an investigator must follow the chain of proxies back. One way is to break into each system until the attacker's system is identified. There the analyst is able to collect information about the attack and person. A different, often unpractical way, for an investigator is to subpoena her way through the proxy chain. However, because of different jurisdictions this is tedious, sometimes even impossible, and most of the time takes too long to catch an attacker red handed or even at all.

2. Stealing back data an attacker gathered, e.g. via a trojan Criminals are using so-called dropzone systems to collect stolen information, such as user credentials, online banking credentials, and documents. These dropzones can be readily identified by analyzing the malicious software. However in order to "get the data back", i.e., determine what data has been compromised and act accordingly, it is often necessary to exploit vulnerabilities within the dropzone software to get access to the system. However, again the legal basis for this is unclear, because especially private investigators would be using unauthorized access in violation of some law. Further again the problem of jurisdiction makes this approach difficult to judge legally.

3. Sinkholing malicious systems IT security researchers are using a technique called "sinkholing" to redirect malicious traffic originally sent to a so-called command and control (C&C) server, to a sinkhole, i.e. a system that analyzes and rejects bad traffic. However, legally this could, in some jurisdictions, be violating telecommunication laws, because the original traffic is diverted, i.e., intercepted.

4. DoS against attacker's controlled systems The most common attack type on the Internet are denial of service (DoS) attacks. In a DoS attack a malicious entity overloads the service provider with bogus request so legitimate users are denied access to the service. A very simple idea to interrupt the operations of attackers is to use a DoS attack against them. However, there is no explicit legal basis for self-defense on the Internet, hence, such actions, especially when interrupting the service of infrastructure not belonging to the attacker, e.g., intermediate routing networks between the attacker and the investigator, can make these actions just as illegal as the operations of the attacker.

5. Blacklisting and blocking of malicious systems Another simple way to stop malicious operations is to blacklist and block the systems used to facilitate them. An example for this are the various blacklists for web servers sending spam emails. However, sometimes spammers use legitimate mail servers or networks of hosting providers for their activities. It thus often happens that the mail or hosting providers IP range is blacklisted, even though the mail or hosting provider has already removed the malicious user from their service. This can lead to DoS against the mail or hosting provider. Legally there are no clear guidelines to whether or not a service provider, here the mail providers receiving mail from a blacklisted system, has the right to freely choose whom he provides service to or not. However, this clearly violates net neutrality.