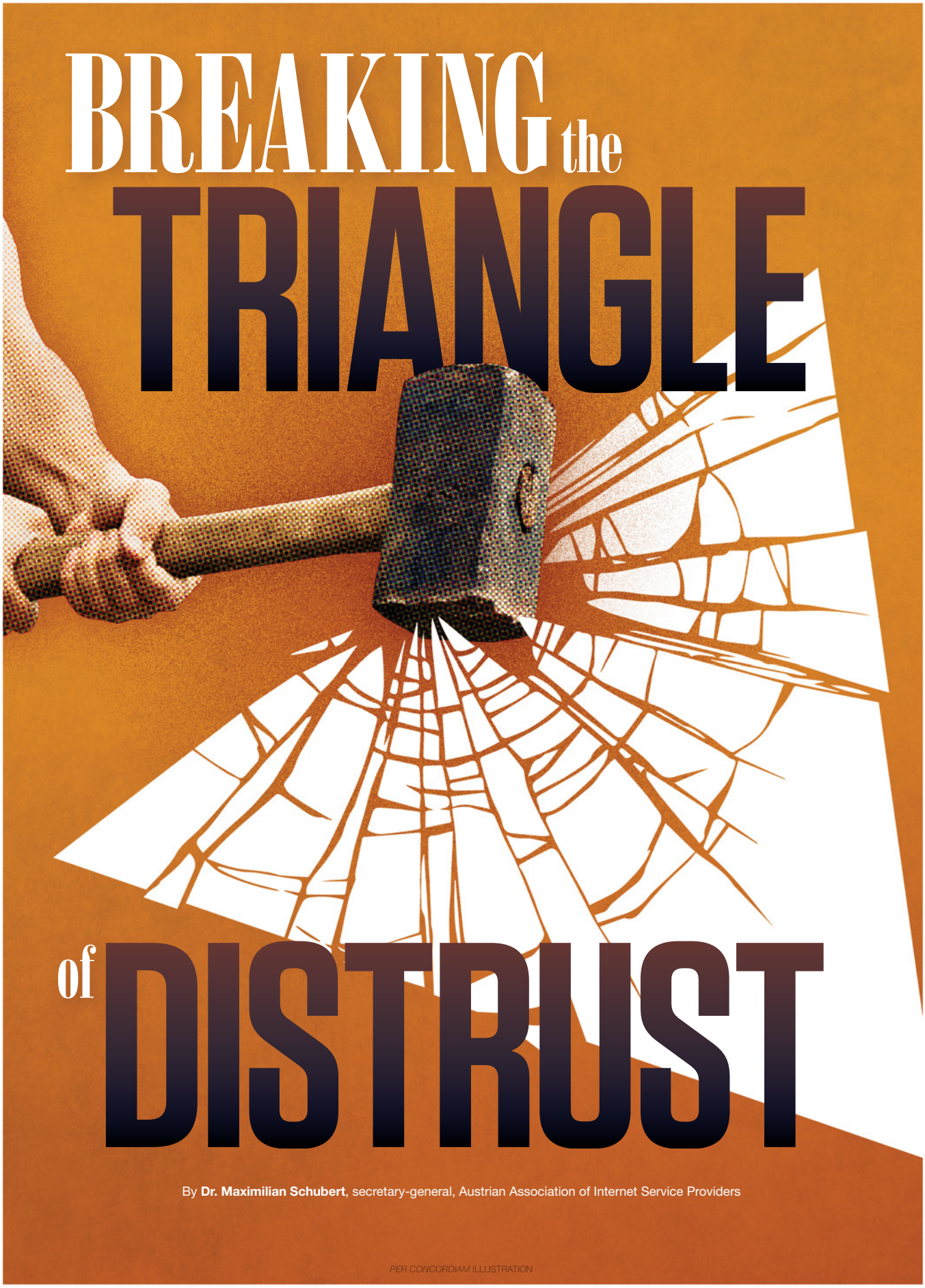
BREAKING the TRIANGLE of DISTRUST



By **Dr. Maximilian Schubert**, secretary-general, Austrian Association of Internet Service Providers

PER CONCORDIAM ILLUSTRATION

Mutual respect and trust are prerequisites for mastering cyber security challenges

For more than 20 years, the majority of online activity was seen as positive, empowering and sparking many beneficial changes for society. Unfortunately, today some people are abusing this technology. Internet service providers (ISPs), law enforcement authorities (LEAs) and civil society have the common goal of making the internet a safer place. However, they address the challenges from different angles: LEAs want to catch criminals, ISPs want to satisfy their customers' needs, and civil society wants to advocate for fundamental rights.

This article builds upon the author's experience as a participant in the Program on Cyber Security Studies (PCSS) at the George C. Marshall European Center for Security Studies in 2017. It aims to illustrate the necessity of a trustful collaboration among stakeholders and tries to outline existing biases.

When attending programs such as the PCSS, it's a great challenge as an industry representative to speak for the whole industry because on most topics there is no common view. Most people might wrongfully assume that the majority of people working in the internet industry share similar cultural views. In reality, cultural and historical influences have a strong effect on their views. For instance, while people originating from established democracies (e.g., the United Kingdom) tend to demonstrate a relatively high level of trust in public institutions and thus might accept a larger degree of public surveillance, people from countries with current and historical reasons to distrust authorities (e.g., Chile) might be significantly more sensitive in respect to privacy and public surveillance.

In the context of the PCSS workshop, the internet industry has been repeatedly criticized for not cooperating sufficiently and has been characterized as contributing to the problem more than the solution. In the discussions it was also evident that many political, social and economic problems were simply projected onto industry. Often, sweeping allegations were made, and it was proclaimed that industry was not willing to "do their bit." It was then seen as almost inevitable that control would be shifted toward government either through increased regulation or a takeover of central functions by public authorities.

A lack of trust was also seen as a factor that is hampering the public sector in its "war for talent." State actors often feel disadvantaged compared to the private sector in respect to their attractiveness as employers, due in part to their rigid employment requirements, salary schemes and confidentiality policies. However, public employers could become highly inventive to obtain desired human resources: While some rely on emotional bargaining, others offer their staff attractive job descriptions, as well as extensive training possibilities and sufficient time in an extremely fast-moving industry to be able to work in detail on technical challenges that arise.

Ideological Differences in a Simulation Game

The tension between privacy, on the one hand, and security, on the other, was a subject that was often raised, but sadly never comprehensively dealt with. The diverging views on this topic were best highlighted within the context of an online simulation game known as CounterNet, a single-player, web-based game focused on how terrorists use the internet and social media for various illicit ends. In this game, players assuming the role of a public authority representative are tasked with tracking and ultimately preventing an attack by a fictional eco-terrorist group. At one point in the game, level advancement was contingent on ordering the observation of the telecommunications of a suspected criminal without a legal basis, thereby knowingly ignoring and intentionally violating fundamental rights. The decision not to give this order resulted in a deduction of points in the game and stopped the player from moving forward to the next level.

During the debriefing, this requirement to break the law triggered a heated debate. While a substantial number of participants refused to act without a legal basis, others showed sympathy for the need to disregard fundamental rights based on the game's scenario of an imminent terrorist attack. As such the simulation did an excellent job, showcasing the different ideologies and attitudes of the various stakeholders and allowing ample time to have an in-depth discussion.

An analyst reviews social media data at the Statewide Information and Analysis Center in Salt Lake City, Utah.
GETTY IMAGES

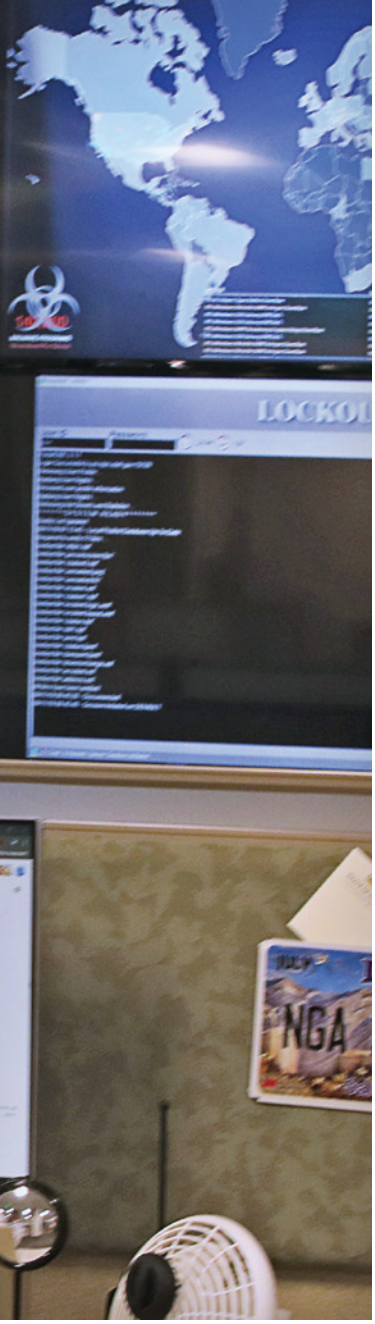
The Triangle of Distrust

It is not an exaggeration to say that the current relationship between industry, civil society and government agencies around cyber security invokes conflict and misunderstanding. But to achieve the common goal — create a "safe" cyberspace — all actors are dependent on each other. While in the past it has often been sufficient for public authorities to rely on their constitutional authority, in the era of "fake news" and targeted national disinformation campaigns, public actors, such as the military and law enforcement, are under more pressure than ever to justify their actions. These doubts should be met with transparency and a willingness to debate openly.

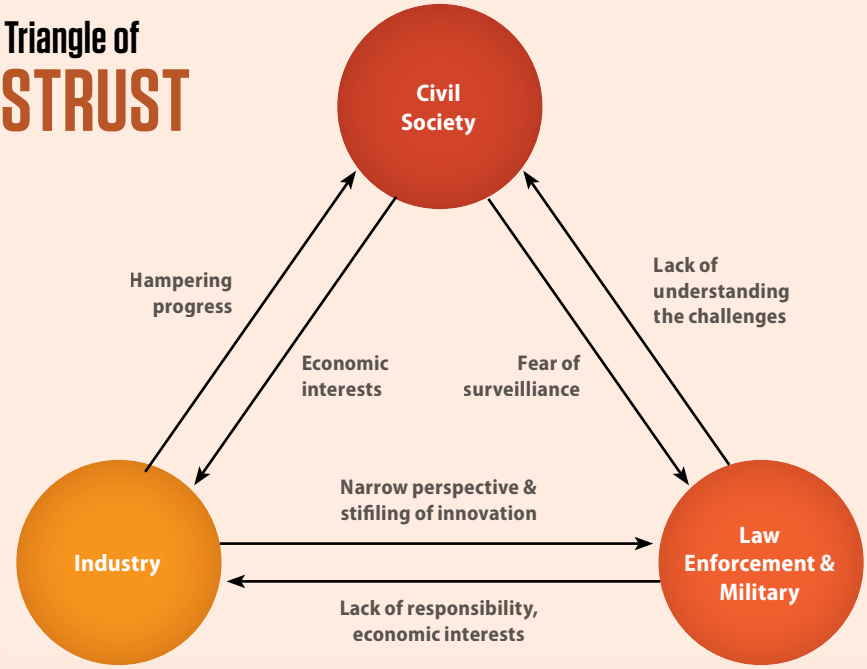
As long as the three stakeholders of civil society, industry and the public sector (LEAs and the military) keep accusing each other in a blanket and polarizing manner, there will be a lack of mutual respect. Such accusations impede the creation of trust, which forms the basis for the necessary cooperation between all actors that is required to tackle the challenges of the cyber realm. To break down the individual elements of this triangle of distrust, the most common prejudices can be summed up as follows:

Civil society distrusts industry for not being transparent about its motives and the degree of its cooperation with law enforcement. Due to necessary secrecy and a subsequent lack of information available to members of civil society, law enforcement and the military tend to be perceived as institutions exaggerating dangers with the aim of extending their influence and control, thereby threatening civil liberties and, effectively, the democratic system.

Law enforcement and the military accuse civil society of being naive and refusing to accept the reality of challenges in the cyber realm. Industry is criticized for not accepting responsibility for the threats they create, while at the same time using the argument of fundamental rights



The Triangle of DISTRUST



not to cooperate with law enforcement.

Industry criticizes civil society for overreacting in respect to privacy and thereby hampering innovation. Law enforcement and the military, at the same time, are sometimes perceived as acting with an overly narrow mindset, ignoring the negative effects their actions could have on business or the further development of the internet and other technologies.

Precisely for these reasons, initiatives such as the PCSS program represent an essential opportunity to identify biases and to subsequently be able to overcome them. To support this process, further expanding the circle of potential program participants should be considered, and representatives of civil society should also be included alongside those of industry. This could help contribute to reducing prejudice among these actors, in addition to establishing greater understanding of the identified prejudices on the part of the military and LEAs.

Trust is a prerequisite for successful cooperation between the internet industry and law enforcement agencies.

While cooperation between industry and LEAs has often been perceived as suboptimal, significant improvement has been achieved by addressing the root causes. Aside from legal and regulatory challenges, surprisingly these are often practical and actionable challenges, as demonstrated by the latest Europol SIRIUS report on cross-border access to electronic evidence, which revealed the most common practical challenges.

The most common challenges for LEAs include not knowing where to turn, not fulfilling the formal requirements (e.g., missing signatures), not providing necessary information (e.g., no valid legal basis) and not knowing how to transfer requests (e.g., LEA insists on sending fax messages instead of emails). To address these issues, a number of European countries, such as the Netherlands, have established specially trained and equipped, national single points of contact for the exchange of information with the internet industry, which has led to a significant rise in successful requests. Another key to their success is the ability to develop a trusted relationship with industry. It can be initiated, for example, by attending the same events as industry members or by inviting them to informal breakfast meetings to discuss practical challenges.

As such, tackling the practical challenges has enabled a new level of cooperation, showing that in almost all cases when ISPs are asked to provide information, a "no" from an ISP does not mean they do not want to help LEAs, but they are not able to help due to technical aspects or legal requirements.

To overcome the differences, while aiming to create a safer cyberspace, serious discussion is needed. Irrespective of how frustrating and resource-draining such a discussion may appear, it may not be bypassed. The PCSS program and the Marshall Center could play a key role in enabling the various stakeholders to build the trust needed to achieve their common goal: a safer internet for every user. Even if opinions about certain topics will differ in the future, a trustful relationship between ISPs, LEAs and civil society facilitates knowledge transfer to obtain this common goal. □