**Internet Governance Forum**
**Proposal for an OECD Open Forum on**

# PRIVATE SECTOR "HACK BACK": WHERE IS THE LIMIT?

The private sector has, in recent years, been exposed to an exponentially increasing number and variety of attacks in the digital environment and businesses are dependent on their respective governments if they wish counter-offensive action be legally taken against attackers. With practices known as "hacking-back" being within governments' prerogative only, how far should businesses be allowed to go in taking proactive defensive measures (also referred to as "active cyber defence")? Should public policy evolve, in order to clarify the conditions, limits and safeguars for private sector to resort to such techniques?

**Key questions**

- What renders a digital security measure as "active" rather than "passive"? What are concrete measures that might fall into each category? Is this categorisation necessary? What is a technology neutral description of "active cyber defense"? Where are the boundaries between "hacking back" and "active cyber defense"?
- What is the prerogative of governments in responding to an attack and where does the scope of action of a business start and ends? Could anyone use proactive defence measures or should only "qualified" players be allowed to enter this space? Should there be any oversight?
- What are the limits of "active cyber defense"? How would what is acceptable and what is not be determined?
- What are the risks of hacking back, including to the Internet and other users? Is there any way to mitigate those risks? Who would be responsible in case of damages to a third party?
- Is there a need for internationally agreed rules and principles in this area?

The lines separating passive from active measures, and active measures from hack-back practices are rather blurred, and government directives concerning the legal frameworks in which private actors can operate are equally vague. Therefore, companies find themselves in a legal grey zone when it comes to reacting to attacks.

The notion of proactive defence encompasses a set of measures one can take beyond usual passive digital hygiene practices and can prove useful in operational digital security risk mitigation. There are many nuances and variations in what terms such as "active defense" and "proactive approach" mean. These range from preventive digital security checkups to luring attackers into extracting infected files to compromise and access their networks to be able to attribute the attack to an individual or a group, and to discourage future attacks and minimise the impact of the current attack. Indeed, as they increase in aggressiveness, proactive techniques become more controversial and are more likely to be considered as being beyond a business's scope of action.

However, proactive defence has also been hailed as an effective tool on which the private sector can rely upon to respond to incidents without resorting to illegal practices, but its use can also bring up a myriad of possibly negative consequences. The attribution problems linked to the digital environment and the interconnectedness of businesses and other internet users significantly increase the probability of collateral damage on third parties. Further, the often transnational nature of these attacks may have political and diplomatic consequences that go beyond anything intended by companies that are simply looking to actively protect their systems or retrieve stolen data amongst other things (e.g. disturbance of law enforcement operations, wars of attrition between attackers and retaliating victims, etc.).

This session will also consider hacking back and proactive defense measures in light of other potential categories of responses to a digital security incident, such as partnerships among the private sector (especially digital security service providers), the government and other stakeholders to share information on threats, attackers' intrusion methods and intentions, co-operating on malware analysis, collaborate in human resource development and training, etc.

Has the time come for new rules and guiding principles to clarify businesses' scope of action, and to allow them to pursue a proactive defence approach of towards their systems and data in an ever increasingly digital and data-driven world?