



# Kaspersky Interactive Protection Simulation (KIPS): technical attribution

---

Contributing  
to cyber-stability  
through capacity-  
building

# Kaspersky Interactive Protection Simulation: technical attribution edition for cyber-stability through capacity-building

## What is KIPS?

**Kaspersky Interactive Protection Simulation (KIPS)** is training that places players into a simulated environment where they face a series of unexpected cyber threats, while trying to maintain confidence.

In **KIPS**, players are supposed to build a cyber defense strategy by making choices among the best pro-active and re-active controls available. Every reaction (step) made by players to the unfolding events changes the way the scenarios play out, and ultimately how close players come toward victory or defeat.

## What is KIPS on technical attribution?

**KIPS training on technical attribution is a ‘detective’ learning exercise.** It simulates a scenario where participants – playing diplomats – face an attack on the UN First Committee, which deals with matters of disarmament, global challenges and threats (including in cyberspace), and maintaining world peace and international security. Players face several cyber events and are provided with the profiles of five threat actors – but only one of them is the culprit conducting a sophisticated targeted attack against UN infrastructure.

The technical attribution edition aims to teach players about the complexities of technical attribution; i.e., it is technical malware analysis. Action cards played and thus decisions made by players through five turns will either lead them to the most accurate technical analysis and help understand who is the culprit by collecting technical pieces of evidence, or will spark greater uncertainty and cyber-instability if the riddle is not solved.

“Capacity-building helps develop the skills, human resources, policies, and institutions that increase the resilience and security of states so they can fully enjoy the benefits of digital technologies.”

The Final Substantive Report of the UN OEWG, adopted by 193 UN Member States on March 12, 2021

# Why KIPS is an effective exercise?

**KIPS training on technical attribution** is targeted at experts in the field of cyber diplomacy, cybersecurity policy researchers and all other practitioners who want to increase their knowledge and awareness of the complexities of technical attribution as well as of the security problems and risks arising from the use of ICTs in the context of international security.

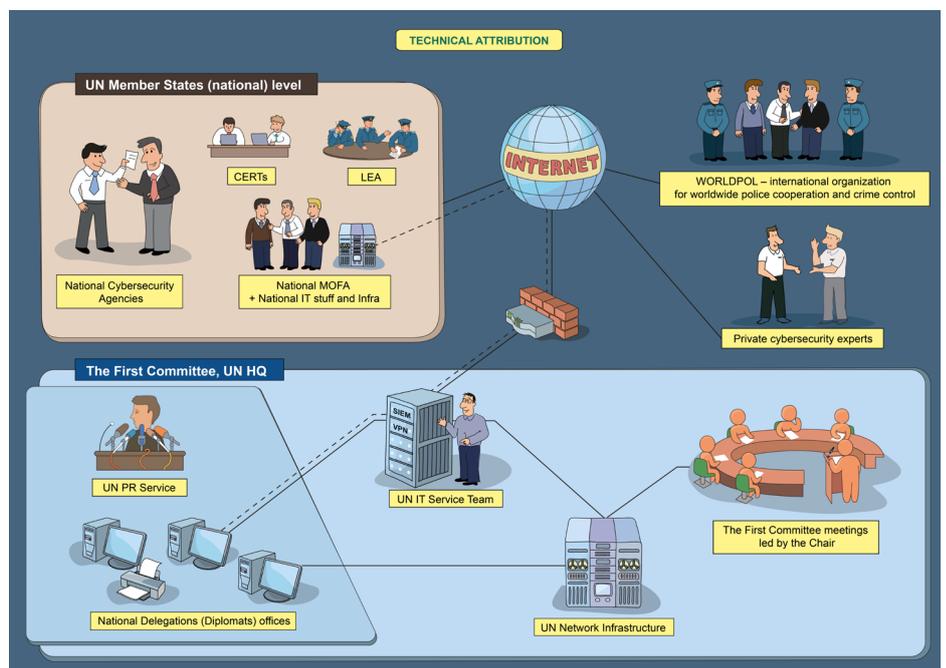
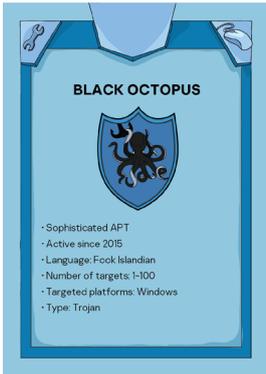
Balancing international security, national security and engineering priorities against the cost of a realistic cyberattack, the players analyze data and make strategic decisions based on ambiguous information and limited resources – just as in real life.

The KIPS training or game is a dynamic awareness program based on 'learning by doing':

- fun, engaging, and quick (two hours);
- teamwork builds cooperation;
- competition fosters initiative and analysis skills;
- gameplay develops a better understanding of cybersecurity measures, risks and complexities of technical attribution.

During the KIPS game, players will learn that:

- technical attribution is a complex process, and its accuracy depends on multiple factors and technical evidence;
- cooperation with other actors, including the broader multi-stakeholder community, as well as exchange of information, is essential for successful cybersecurity work.



# How is KIPS training organized?

KIPS training on technical attribution is organized into two formats: live and online.

## KIPS online

- Two-and-a-half hours: the game and the allocated time for discussion of the lessons learned as well as for explaining how the best scenario should have been played
- Up to 300 teams simultaneously, from any location
- Teams can choose the game interface in a different language
- A trainer leads the session via WebEx or Microsoft Teams

## KIPS live

- Two-and-a-half hours: the game and the allocated time for discussion of the lessons learned and for explaining how the best scenario should have been played
- Up to 80 trainees in the same room\*
- The same language for all participants
- A trainer and an assistant on site
- Printed materials provided

---

\* Once the global health situation permits the gathering of such large groups.