Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

20 June 2024

Initial NCSC review of the work of the Cyber Situation Network formed for the Summit on Peace in Ukraine

The Summit on Peace in Ukraine took place on 15–16 June at the Bürgenstock resort and was attended by delegations from almost 100 countries. The possibility of cyberattacks targeting the event and network infrastructure in Switzerland had been anticipated in the run-up to the summit. There were indeed a number of cyberattacks, but all were detected early and quickly averted. This report by the National Cyber Security Centre (NCSC) provides an initial assessment of the performance of the Cyber Situation Network.

1. Objectives and mandate

The main objectives for cyberdefence were to ensure:

1. **freedom of movement** and readily **available means of communication** for security and emergency personnel;

2. **confidentiality, integrity and availability of the IT resources** of all conference participants and Cyber Situation Network partners;

3. the efficient **flow of information** to where it could provide the greatest operational benefit;

4. a **clear understanding of roles** and **consistent action** among partners.

In addition to its protection mandate, the NCSC took on the overall coordination of the preparation, implementation and follow-up. The Cyber Situation Network consisted of almost 100 experts from national and cantonal authorities and private sector organisations. Each organisation played its part and shared the necessary information with its partners. The mandate was therefore fulfilled and the objectives met.

2. Cyber Situation Network and Cyber Situation Centre

The NCSC, together with the Lucerne Police, opened the Cyber Situation Centre for the Summit on Peace in Ukraine in at the Lucerne Police premises on Thursday, 12 June. This followed weeks of planning and preventative work, including measures to raise awareness of potential targets and to manage the attack surface of critical infrastructure and the organisations concerned.

Cooperation was smooth at all times, thanks to the high level of commitment and thorough preparation of all those involved. The broad support provided by the Cyber Situation Network was crucial in building cyber resilience ahead of the conference and enabling a rapid and effective response to cyber threats during the event.

At the same time, a public awareness campaign was organised under the leadership of the NCSC. The aim was to ensure that all partners were informed as transparently, accurately and quickly as possible about incidents relevant to them. This required continuous updates from the Cyber Situation Network and coordination with partner organisations.

3. Cyber incidents related to the summit

Switzerland experienced a number of cyber incidents shortly before, during and briefly after the summit. The following are particular noteworthy:

- **DDoS attacks on websites of the Confederation and related organisations:** On Thursday, 13 June, the NCSC and its partners detected a series of DDoS attacks clearly attributed to the pro-Russian hacktivist group 'NoName057(16)'. These cyberattacks targeted the public websites of a total of 22 Swiss authorities and organisations. Overall, the DDoS attacks were within the expected range and caused only minor disruption to IT infrastructures. However, at no time was there any threat to the IT systems or data of the summit itself or the organisations involved in its organisation.

- **Hacking attempts on NW/OW cantonal IT systems:**
  The IT departments of the cantons of Nidwalden (NW) and Obwalden (OW) reported hacking attempts on their email systems. An analysis by the NCSC showed that these were opportunistic intrusion attempts and not related to the summit. The hacking attempts were unsuccessful. Together with the NCSC, the cantonal IT department identified and immediately implemented measures to secure the system.

- **Phishing attack against staff of Lucerne's emergency medical call centre (LU):** Shortly before the summit, a suspected cyberattack against staff of Lucerne's emergency medical call centre was reported. Unknown perpetrators are believed to have used fake emails (i.e. phishing emails) to try to obtain employee access details. The cyberattack was recognised as such by employees and reported to the Cyber Situation Network. Thanks to the quick response of employees, the cyberattack was averted at an early stage.

- **A mishap during the FDFA livestream led to rumours of cyberattacks:** After the live broadcast of speeches by President Viola Amherd and Ukrainian President Zelenskyy, members of the interpreting service forgot to switch off their microphones. In the ensuing discussion on the FDFA livestream, they referred to 'technical problems' during the interpretation, with one of them saying that he had warned of cyberattacks in the run-up to the summit. This mishap led to several media enquiries to the NCSC and the FDFA, as well as to reports in some Swiss media about possible (Russian) cyberattacks. However, the technical problems mentioned were not the result of a cyberattack.

- **Power failure in the city of Bern:**
  A power failure in the city of Bern on Sunday morning fuelled rumours of a possible cyberattack. As a result of the blackout, some federal authorities and other organisations based in Bern switched to emergency power. Clarifications with grid operators and electricity companies ruled out a cyberattack as the cause of the blackout.

- **Digital vandalism:**
  Digital vandalism on a publicly accessible portal by an unknown perpetrator led to a temporary disruption of a deployment system. The portal is owned and operated by a Swiss association. The incident was quickly recognised and the 'vandalised' data was immediately removed from the deployment system. At no time was the security of the mission-critical systems or their data compromised.

There were other suspected cyberattacks against the summit security system. In each case, swift action was taken. No further information on these attacks will be released at this time. However, as a result of the measures taken, these attacks did not compromise the security or proceedings of the summit at any time.

4. General

The NCSC disbanded the Cyber Situation Network on Sunday, 16 June 2024.
On 20 June 2024, the BACS was still detecting individual DDoS attacks on targets in Switzerland. It can be assumed that the situation will normalise again in the coming days.