(DRAFT v01.10) – 25 September 2025

The IRTF is the sister organization of the IETF standards organization. The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organization, the Internet Engineering Task Force (IETF), focuses on the shorter-term issues of engineering and standards making.

The IRTF is comprised of a number of focused and long-term Research Groups. These groups work on topics related to Internet protocols, applications, architecture and technology. Research Groups have the stable long-term membership needed to promote the development of research collaboration and teamwork in exploring research issues. Participation is by individual contributors, rather than by representatives of organizations.

See IRTF.org

Proposal for a new Research group in the IRTF (called PAIN-P)

Proactive Analytics and Intelligence for Network Protection (PAIN-P) RG

Background

In the past few years, significant advances have been made in data analytics and computational social science, leading to the recent re-excitement in Artificial Intelligence. Computational data analytics approaches are making their way into different aspects of the digital economy. These have focused primarily on enterprise/organizational business data and on consumer behavior analytics post-event.

However, there remain considerable opportunities for these data analytics and AI techniques to be used proactively to address network security defenses. The recognition of the potential role of AI in cybersecurity is reflected in the recent White House Executive Order (EO) of June 6th, 2025 (Section 5) on *Promoting Security with and in Artificial Intelligence*.

These opportunities include the (i) fast detection of attempted attacks into organization networks and ISP networks, (ii) immediate adjustment of the security posture of the network in response to perceived attacks, and (iii) continuous monitoring and correlation with events occurring outside the organizational boundary (e.g., attacks on other networks).

In order to explore how these data analytics and computational intelligence techniques can be utilized to improve network cybersecurity practices, the current document proposes a new Research Group (RG) in the IRTF called the Proactive Analytics and Intelligence for Network Protection (PAIN-Protection) research group. The main goal of this RG is to identify open problems, share research results, and explore how the research efforts can be utilized to improve network security.

Some of the topics of interest in PAINP RG include (see Figure 1), but not limited to:

- Trends in data analytics and computational intelligence that may impact network cybersecurity.
- Novel approaches to network-driven data analytics system architectures that can improve cybersecurity solutions in enterprises and other organizations.
- Mechanism to communicate intent among AI-based systems across independent networks.
- Approaches to integrate computational intelligence into network architectures.
- Approaches to report and measure the degree of accuracy in the proactive adjustment of the security posture of the network.
- Techniques and approaches for collecting network data while ensuring user-privacy is protected (i.e. no PII leakage).
- Network Behavioral Analytics, and Non-Person Entity (NPE) Discrimination (AI vs Human) Analytics.
- Other topics related to networks, network-data and AI technologies.

Membership

Membership in the PAINP RG is open to all interested parties.

Meetings

The PAINP RG will meet one to three times per year, as deemed necessary by the chairs and according to demand. At least one PAINP RG meeting will be co-located with an IETF meeting per year. Given that the PAINP RG seeks to bridge the gap between Internet standards and AI research communities, the PAINP RG may also meet collocated with relevant academic conferences or network industry forums, as appropriate.

Meetings are by default open with open attendance, with remote participation and recording as provided by the meeting venue, according to the IPR policy of the IRTF.

Proposed Co-Chairs

- Alex Pentland (Stanford)
- Thomas Hardjono (MIT)
- Bruno Lepri (Trento University)

We are seeking a list of Supporters who think that such a Research Group in IRTF would be a useful discussion forum. There are no obligations to write specifications or technical documents. Presentations will be most welcome.

Supporters who think the PAIN-P RG is a good idea (unordered list):

Mark Nitzberg (UC Berkeley)	Suleman Ahmad (Cloudflare)
Ellis Society EU	Carter Bullard (IACD/Johns Hopkins)
Fondazione Bruno Kessler EU	Orie Steele (mesur.io)
Kathleen Moriarty (Security Bias Inc)	Carsten Maple (Alan Turing Institute)
Flemming Andreasen (Cisco)	Alex Weinert (Semperis)
Guy Fedorkow (MIT)	Data61/CSIRO (?)
Nirmal Rajarathnam (HPE)	Jon Green (HPE)
Jon Crowcroft (Cambridge University)	Bob Friday (Juniper/HPE)
Russ Housely (Vigil Security)	…

References

Executive Order on Sustaining Select Efforts to Strengthen the Nations Cybersecurity. https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

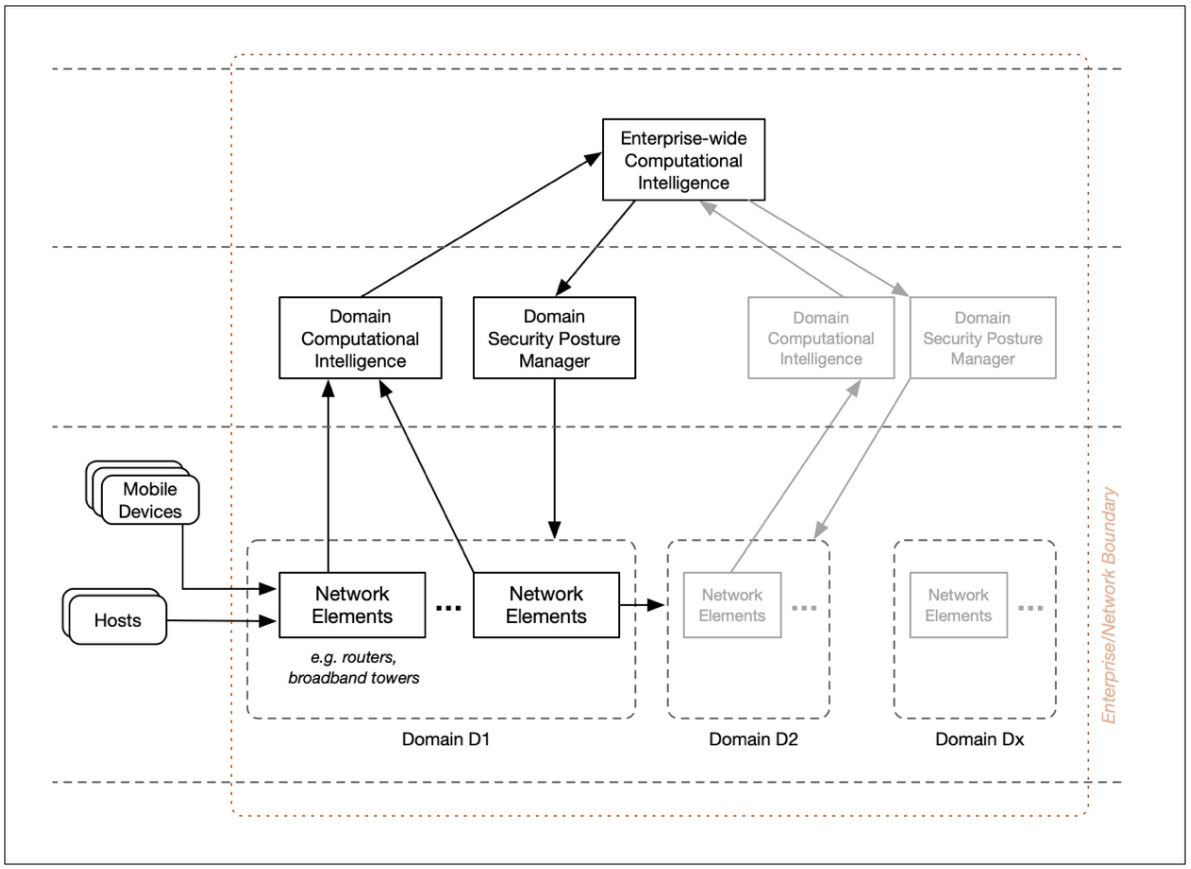
Enterprise-wide Computational Intelligence
Domain Computational Intelligence
Domain Security Posture Manager
Domain Computational Intelligence
Domain Security Posture Manager
Mobile Devices
Hosts
Network Elements
Network Elements
e.g. routers, broadband towers
Network Elements
Network Elements
Domain D1
Domain D2
Domain Dx
Enterprise/Network Boundary

Figure 1