As cyberspace and its residents, human and otherwise, grow in expressiveness, creativity, and energy, it seems inevitable that there will also emerge a growing need for, and development of, regulation. if such regulation is neglected, as we argue it has been up to now, the regulations imposed by nation-states, corporations, and other stakeholders, might cast an unnecessary and unwanted shadow on cyberspace. In this research, we argue that cyberspace needs a social contract, with its entities (individual users, organizations, devices, and service providers), and propose a draft of such a social contract, and develop a methodical security design philosophy that can guarantee enforce and maintain the safety and security conditions, so long as these conditions are consistent with the social contract for cyberspace.

1. Demonstrating that cyberspace needs a social contract and proposing a draft of *a social contract for cyberspace*.
2. Developing a *stakeholder security analysis* which are:
   1. Formulating the safety and security conditions, that are consistent with the social contract for cyberspace, as a statement of the user’s expectations of the system (Netml System).
   2. Analysing the source code of the system to prove that it meets these conditions.
3. Developing *Inference graphs*, a graphical representation of cybersecurity architecture, which assist cybersecurity professionals to define the security objectives of their systems, the rules which enforce this security, and the reasoning behind the choice of these rules.