

## Abstract

Daniel Bilar, University of New Orleans

### \_nth-order attacks\_

The goal of nth-order cyber-warfare is to induce instabilities/failures in mission-sustaining /ancillary/ systems that ultimately degrade the end target. These ancillary systems may - but needn't be - technical systems; ancillary systems include /pars pro toto/ hardware/software manufacturing, economic business model subversion, control algorithm degradation, fault detection/resilience/recovery hindrance, symbiotic leverage of humans-as-code, power generation/transmission/distribution degradation, semantic hacking and more.

For example, a denial of service attack is a case of a 2nd-order attack against the TCP resource allocation control subsystem; Thompson's Trojaned compiler in "Reflection on Trusting Trust" (1984) may be seen as a 3rd order attack against software manufacturing tools. The operational war tactics proposed by PRC General Pan Junfeng in 1996 against US computer systems read like a blueprint for n-th order attacks: Data poisoning, OODA decision loop subversion, banking system and social order degradation.

This paper discusses this class of attacks and tries to explain their etiology via Highly Optimized Tolerance (HOT) models. HOT mechanism are a way of generating complex, structured systems via optimization processes that incorporate tradeoffs between objective functions and resource constraints in probabilistic environments. Pertinent to our discussion is the property that such optimization-generated systems are /robust towards common perturbations, but especially fragile towards rare events/, such as unanticipated changes in the environment. Inducing such 'rare events' in mission-sustaining ancillary systems is thus the goal of nth order attacks. We will illustrate the proposed HOT models with concrete historical, current and forward-looking examples in the context of cyberwar against advanced computerized societies. Finally, we will discuss the challenges, technical and otherwise, for mitigation of such attacks.

### Biography Daniel Bilar

Daniel enjoys figuring out syncretic ways to solve problems. He has degrees from Brown University (BA, Computer Science), Cornell University (MEng, Operations Research and Industrial Engineering) and Dartmouth College (PhD, Engineering Sciences). He was a founding member of the Institute for Security and Technology Studies at Dartmouth College, conducting counter-terrorism technology research for

the US Department of Justice and Department of Homeland Security. He is currently an Assistant Professor of Computer Science at the University of New Orleans. Active research topics include detection, classification and containment of highly evolved malicious software, quantitative risk analysis/management of networks, as well as optimization of business and innovation processes.