An Immune System for Cyberspace as Deterrence

1. Conventional forms of deterrence are unsatisfactory
    a. By-punishment: problematic and risky
    b. By-denial: if denial is good enough to deter, why bother deterring?

2. A third form of deterrence threatens to remove the tools of hackers
    a. Which matters because hackers increasingly count reusing cyber tools
    b. If these tools cannot be used often before being rendered obsolete:
        i. The cost of hacking rises
        ii. The ability to hack a target of opportunity declines.
        iii. Mass attacks start to edge off the table as being too hard to complete before detection leads to roll-back

3. A global surveillance system would have two components:
    a. Distributed sensors designed to find indications of APT attack
    b. Global feedback on signatures of tools
        i. "Tool" is defined to include a spectrum from signatures to social engineering tricks, IP addresses, malware attributes (e.g., that frustrate detection), and novel attack vectors, to zero-day vulnerabilities
        ii. Tools range in the ease with which they can be altered from case to case.
    c. Many issues have yet to be worked out: potential research agenda

4. Where to put the sensors
    a. On the surface? Sees the exploit but may miss most zero-days, misses attacks targeted at named individuals, may see too much that would not have gotten through anyhow.
    b. Sub-surface?
        i. Not the best place to see the zero-day that penetrates outward-facing systems.
        ii. May still see exploits that go from edge to core compromise
        iii. Will only see attacks that breach perimeter
    c. ISPs might host sensors mounted on cloud-based simulated targets
        i. Perhaps a mix of fully-patched and not-fully-patched systems the latter to find the special exploits that work only after initial penetration
    d. Sensor should be an otherwise quiet machine (or at least one that can distinguish expected from unexpected inputs); may need external polling of files/memory for change detection.
    e. How can the work of extracting characteristics of tools from anomalies be scaled? What about from tool characteristics to signatures?
    f. What detection can be engineered against non-malware attacks?
    g. How would hackers try to game the system (both false-positive & false-negative)?

5. Policy considerations
    a. What about limiting the distribution of indicators to those willing to host sensors?
    b. How is success advertised for deterrence purposes?
    c. Need to address PII, transparency concerns.
    d. How to bring networks of friendly countries into the system
    e. Can sensors play roles as IDS for those without IDS systems?
    f. How to keep the *good cooperative* cybersecurity folks happy and making money