Appeasement in Cyberspace: assessing the ethical permissibility of conceding to ransomware attacks

MIDN 1/C Collin P. Kane, U.S. Navy
United States Naval Academy

This research was initiated in response to the growing number of ransomware attacks affecting both the public and private sector, and seeks to propose an ethical framework for stakeholders to consider when assessing their options after an attack. Existing research in the field focuses primarily on preemptive measures to prevent an incident from occurring (cyber ‘hygiene,’ routine backups, etc), but very little guidance has been made publicly available to assist in the decision-making process once damage has been done. Through a consequentialist lens, this research provides deeper insight into potential corollary effects of a given decision based on specific variables surrounding the attack. The ethical permissibility of the decision, then, is dependent upon such variables, which are not limited to the following:

- Government vs. Private Sector
- Sensitivity of data
- Probability of receiving encryption key
- Ability to pay
- Timeliness of attack
- Form of payment
- Entity paying the ransom
- Number of individuals affected

This research is still a work in progress, but it holds value in shifting the dialogue towards a more practical solution for all parties invested in solving the ransomware crisis that is plaguing our businesses every day.