Hacking and Cybersecurity

I. Three kinds of 'hackers'
    A. Black hats
    B. White hats
    C. Grey hats

II. The *prima facie* case against cracking
    A. Moral rights are not absolute, but they do resist social welfare tradeoffs
    B. Property rights
    C. Privacy rights
    D. Economic costs to hacking

III. Weak arguments for cracking
    A. Social benefits
        1. Knowledge about security flaws
        2. Improved insight into computer systems
    B. Avoiding waste
    C. Free flow of information

IV. Hacktivism as civil disobedience
    A. Civil disobedience defined
        1. Public
        2. Conscientious
        3. Violation of the law
            a. Need not be the unjust law itself
            b. Willingness
        4. Non-violent
        5. Attempt to communicate an injustice/pressure social change
    B. Core examples of civil disobedience
    C. Hacktivism as civil disobedience
        1. Standard strategies of hacktivism
        2. Himma's argument against hacktivism as CD
            a. Failure to accept consequences of law violation
            b. Third party damage undermines the claim to CD
                1) Depends upon hacktivist technique
                2) Depends upon type of website
            c. Implausibility of basic values that motivate CD
    D. Flaws in Himma's arguments
        1. What constitutes 'failure to accept consequences'? What about revolutionary contexts where punishment is grossly disproportional?
        2. Civil disobedience always generates costs to innocent third parties
        3. Civil disobedience can be a kind of moral entrepreneurship: being a minority position is common