Notes on: Demchak, C. C., & Dombrowski, P. (2011). *Rise of a cybered westphalian age*. Strategic Studies Quarterly.

J MacCormick, Spring 2013

## Introduction

- Stuxnet marks a turning point in the way that states view the potential for cyber conflict:
  - "Until Stuxnet, however, it was not entirely clear if all the access points, malware, and rampant penetrations would lead to serious strategic harm. The consensus among states changed after Stuxnet." (p33)
- As a result, states will increasingly act to protect their own zones of cyberspace:
  - "A new 'cybered Westphalian age' is slowly emerging as state leaders organize to protect their citizens and economies individually and unwittingly initiate the path to borders in cyberspace." (p35)

## The "Westphalian" Process

- What does "Westphalian" mean?
  - Refers to some European treaties in 1648
  - "After the Westphalian peace, the nation-state became the dominant form of social organization. As a result, leading states of the period helped codify and set about more or less enforcing a collectively agreed upon set of rules, institutions, and norms by which they interacted with each other in international society" (p37)
- Perhaps the historical processes behind the evolution of Westphalian borders can help us understand what will happen in cyberspace

Interesting claim: "The modern state intends to put in place a buffer, a bulwark, a way to buy the nation time to respond if attacked. In short, they are iterating toward national borders in cyberspace to relieve the pressure of the barrage of assaults" (p39). What is their evidence?

## Practical Reinforcement—Borders Decrease the Ease of Cybered Offense

- This section seems to make the point that erecting a border in cyberspace makes it more difficult for outsiders to attack
- Is this a tautology? Is there a more subtle point?

## Virtual Borders—Feasible, Comfortable, and Manageable

- Meaningful national borders within cyberspace are technologically feasible:
  - "It is technologically possible for governments to require source tagging of bytes at some point to assure the passage of legally acceptable streams of data or applications or volumes of requests as a way to curtail attacks on their soil or emanating from their soil illegally." (p41) *Do we believe this? See discussion of China, p42 and pp45-47.*
- Borders are understood by ordinary people and existing international processes respect them

## Emergent Virtual Borders

- Evidence for emerging borders is seen in
  - Government filtering and surveillance (p45)
  - Regulation of communication companies (p47)
  - Formation of military cyber commands (p48)

## Cyber Command—The US Model

- Discusses the mission of US Cyber Command
- Mentions the influence of the creation of US Cyber Command on other countries:
  - "For the United States to announce a new national cyber command automatically provokes a new debate in the international military and legal communities" (p49)
- Three important features are:
  - Cyber Command is a *military* unit
  - Blends offensive, defensive, and intelligence-gathering functions
  - Straddles the standard military divisions (Army, Navy, Air Force)

## Resuscitation of International Relations Theory and History

- Claims that the standard theories of international relations will help in understanding countries' interactions in cyberspace:
  - "With the establishment of borders in cyberspace, everything we know about deterrence, wars, conflict, international norms, and security will make sense again as practical and historical guides to state actions and deliberations" (p54)

## Conclusion

- Predicts international agreements on cyberspace:
  - "In the near future, states will delineate the formerly ungoverned or chaotic cybersphere by formal agreement." (p57)
- Emphasizes the notion of national cyberspace accountability:
  - "in much the same way as they operate today in the physical world, attacks across borders will become state responsibilities, whether or not the state approves or guides the attacks" (p57)