

Thema der Sequenz:

Gute Cybersicherheitspolitik im 21. Jahrhundert – Politik der Abschreckung und Alleingang oder Resilienz und Gemeinschaft?

Hauptintention der Sequenz:

Die Schülerinnen und Schüler erwerben die Fähigkeit Strategien der Cybersicherheitspolitik hinsichtlich ihrer Effektivität differenziert beurteilen und dabei das eigene Verständnis von guter Sicherheitspolitik (Sanktionen/ Abschreckung vs. Resilienz/ Prävention und nationale vs. internationale Lösungen) reflektieren zu können.

Thema	Inhalt
Cyberangriffe – aufgebauschte Sicherheitslücke oder unterschätzte Bedrohung unserer Gesellschaft? <i>Die SuS können die Anfälligkeit des Cyberraums hinsichtlich seiner Bedrohungslage differenziert (Sicherheit, Wohlstand, Stabilität) beurteilen.</i>	Gefahren/ Auswirkung von Cyberangriffen Aktuelle Beispiele (Problembewusstsein schaffen)
Konfliktfeld Cyberraum – eine neue Herausforderung der internationalen Sicherheitspolitik? <i>Die SuS können die Konfliktfelder des Cyberzeitalters hinsichtlich ihrer Form (Art, Vielschichtigkeit) differenziert (nicht grundsätzlich neu/ cybered conflict vs. neue Art/ cyber conflict) beurteilen.</i>	Umfang - Raum, Zeit, Kräfte - und Mittel von Cyberangriffen, hybride Bedrohungen (Probleme identifizieren: Auf was soll reagiert werden? Womit haben wir es zu tun?)
Cybersicherheit – Sicherheit für den Nationalstaat oder individuelle Sicherheit? <i>Die SuS erwerben die Fähigkeit den Sicherheitsbegriff differenziert (traditionelle nationale Sicherheit vs. menschliche Sicherheit/ gesellschaftliche, ökonomische und politische Sicherheit) beurteilen und dabei den eigenen Sicherheitsbegriff (eindimensional vs. mehrdimensional, ggf. auch positiven und negativen Friedensbegriff) reflektieren zu können.</i>	Maßstäbe für Cybersicherheit (Ziel von Cybersicherheitspolitik definieren)
Androhung von Strafe – einfachste Lösung zur Abschreckung? <i>Die SuS können exemplarische Sanktionen (z.B. IT, wirtschaftlich, militärisch) differenziert (Umsetzbarkeit und Legitimation vs. Effektivität) beurteilen und dabei ihr eigenes Leitbild guter Sicherheitspolitik verdeutlichen (Machtpolitik vs. Diplomatie).</i>	s.o. z.B. „Hack-back“, Urheberproblematik, völkerrechtliche Grundsätze
Internationale Normensetzung – Schutz des eigenen Staates oder kein Ausweg aus dem Sicherheitsdilemma? <i>Die SuS erwerben die Fähigkeit zur internationalen Normensetzung als Handlungsoption differenziert (absolute vs. verbesserte Sicherheit) und reflektiert (nationale vs. internationale Strategien) Stellung nehmen zu können.</i>	s.o. z.B. Beschränkung von Cyberfähigkeiten, Ächtung, völkerrechtliche Einordnung, Sicherheitsdilemma, „naming and shaming“
Die EU–Strategie zur Cybersicherheit – Sicherheit durch Resilienz? <i>Die SuS können ausgewählte Maßnahmen der Cybersicherheitsstrategie der EU hinsichtlich ihrer Effektivität (auch bzgl. Zeithorizont) differenziert beurteilen und das eigene Verständnis von Cybersicherheitspolitik (Resilienz/Prävention/ defensive Sicherheitspolitik vs. Abschreckung) reflektieren.</i>	Handlungsoption am Beispiel (Lösungsansätze hinsichtlich Zweck- und Wertrationalität prüfen) Technische und organisatorische Vorsorge, offensive Cyberfähigkeit
Eigene Strategien entwickeln – welche Option ist die bessere? <i>Die SuS entwickeln begründet und unter Heranziehung selbstgewählter Kriterien eine eigene Handlungsstrategie und verdeutlichen dabei ihre eigene Vorstellung von Frieden und Cybersicherheitspolitik.</i>	(Lösungsansätze auf Grundlage individueller Zweck- und Wertrationalität entwickeln)

