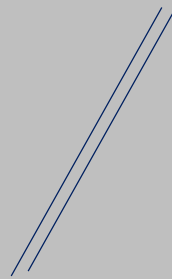


FAKE VERSUS
FAKTEN



LITIGATION-PR IN
DER POST-TRUTH-
ÄRA

Litigation PR Tagung Schweiz
Winterthur, 18.4.2018

Naima Strategic Legal Services &
Schneider Minar Jenewein Consulting



CRISIS & LITIGATION COMMUNICATORS
ALLIANCE

Über uns

Schneider | Minar | Jenewein

LITIGATION CRISIS CAMPAIGNING

SMJ Consulting ist eine europäische Boutique Agentur mit Sitz in Wien und London. Wir arbeiten global und managen für unsere Kunden kritische Situationen. Seit 2007 am Markt, sind wir vor allem im Bereich strategische Rechtskommunikation zu Hause.



NAİMA Strategic Legal Services ist ein hochspezialisiertes Kommunikationsunternehmen, dessen Kernkompetenz in der strategischen Rechtskommunikation (Litigation-PR) liegt. Wir entwickeln komplexe Kommunikationsstrategien für Unternehmen, (NG-)Organisationen, Verbände, deren Spitzenvertreter sowie für prominente Persönlichkeiten aus Wirtschaft, Politik und Entertainment, die sich vor oder bereits in einer juristischen Auseinandersetzung befinden.



CRISIS & LITIGATION COMMUNICATORS
ALLIANCE

Die Crisis and Litigation Communicators' Alliance (CLCA) ist ein internationales Netzwerk von unabhängigen, eigentümergeführten PR Beratungen, die im Bereich Litigation PR und Krisenkommunikation tätig sind. Der Vorsitz der CLC Alliance liegt seit 1.1.2018 bei SMJ Consulting in Wien.

Fake News – nicht neu, aber neuartig

- „Fake News“ sind nicht neu – es gab vergleichbare Phänomene immer.
- Historische Beispiele gibt es zahlreiche zB. Emser Depesche, Französische Revolution, Irak Krieg 2003.
- Allerdings: Phänomen eher auf den Bereich strategische politische Kommunikation begrenzt. Heute erstmals breite Diskussion.
- Neue Herausforderungen für die Wirtschaft.
- Sprachliche Verwirrungen rund um Fake News sind zahlreich – eine Einordnung bietet das Schema rechts.



Digitaler Durchlauferhitzer

Katalysatoren für Fake News liegen vor allem in der Digitalen Kommunikationskultur und deren relativ neuen Ausprägungsformen.

- Zeit der «**Daueraufregung**» und des «**permanenten Skandals**» (vgl. B. Pörksen)
- **Moralische Überhöhung**
- **Geringe Eintrittsbarrieren** (v.a. Kosten)
- **Aufmerksamkeitsökonomie** (Engagement bei negativen/emotionalisierten Themen um Faktor 6 höher)
- Problem der **Communities/Filter Bubbles**, «was wo ankommt»
- Digitaler Einfluss manifestiert sich später in der «offline» Realität.



Aber was hat das mit Unternehmen zu tun?

Es gibt eine Reihe von Akteuren, die sich – in gewissen Situationen – einen Vorteil durch die Anwendung von Desinformation verschaffen.

Eine erste Studie (**Desinformation, Lage – Prognose und Abwehr**) vom Herbst 2017 zeigt, dass die Problematik existent ist, Sicherheitsexperten allerdings noch kaum Strategien entwickeln konnten.

Auslöser für Desinformation(skampagnen) können etwa sein:

- Ehemalige, verärgerte Mitarbeiter (Rache)
- Konkurrenten (Marktanteile)
- Investoren, Corporate Raider (feindliche Firmenübernahmen)
- Hedgefonds, Leerverkäufer (Aktienspekulationen)
- Anlegerschutzanwälte (Mandatsfänger)
- NGOs (Veränderungen erzwingen)
- Whistleblower (Missstände aufdecken)
- Beeinflussung von juristischen/behördlichen Verfahren



Betroffene Bereiche & Schadenspotenziale

Unternehmerische Bedrohungsbereiche

- Produktionsprozesse & Qualität (zB Verunreinigungen, Minderwertige Qualität)
- Kunden & Lieferanten (Kundenbeschwerden, Sourcing von bedenklichen Quellen, oder ethisch abzulehnende Partnerschaften)
- Mitarbeiter & Management (Arbeitsbedingungen, Management-Pfründe)
- Finanzen und Legal (Liquiditätsengpässe, Überschuldung, Compliance Verstöße)
- Event-Bezug (M&A Situation, Produkteinführung, IPO...)

Möglicher Impact auf

- Unternehmensreputation (Arbeitgeber/mediale Reputation)
- Aktienkurs
- Behördliche Verfahren
- Marktanteile



Wie kann ein Angriff strukturiert sein?

Identitätstäuschungen

- **Eine Person** die mit einer «fake» oder «gestohlenen» Identität ausgestattet ist
- **Ein Netzwerk von Personen** die mit anonymer oder gestohlener Identität ausgestattet sind – teils kooperieren (Trolle)
- **Automatisierte Profile** die automatisch an Diskussionen teilnehmen (Bots)

Verbreitungsstufen

- Stufe 1: **Prägung der «Wahrheit»** (Fake Facts)
- Stufe 2: **Verbreitung der «Wahrheit»** (Interaktion, Likes, PR, Tweets)
- Stufe 3: **Ewiges Gedächtnis** (Wikipedia, digitale Archivfunktionen)



Quelle: Bellingcat.com
David Jewberg

Case Study – Feini, Feini, die Babynahrung



Abwehr kommunikativer Attacken: Aktivitätsebenen

Detection



Forensic



Communication



Legal



Digital



Wie kann eine strukturierte Herangehensweise aussehen?

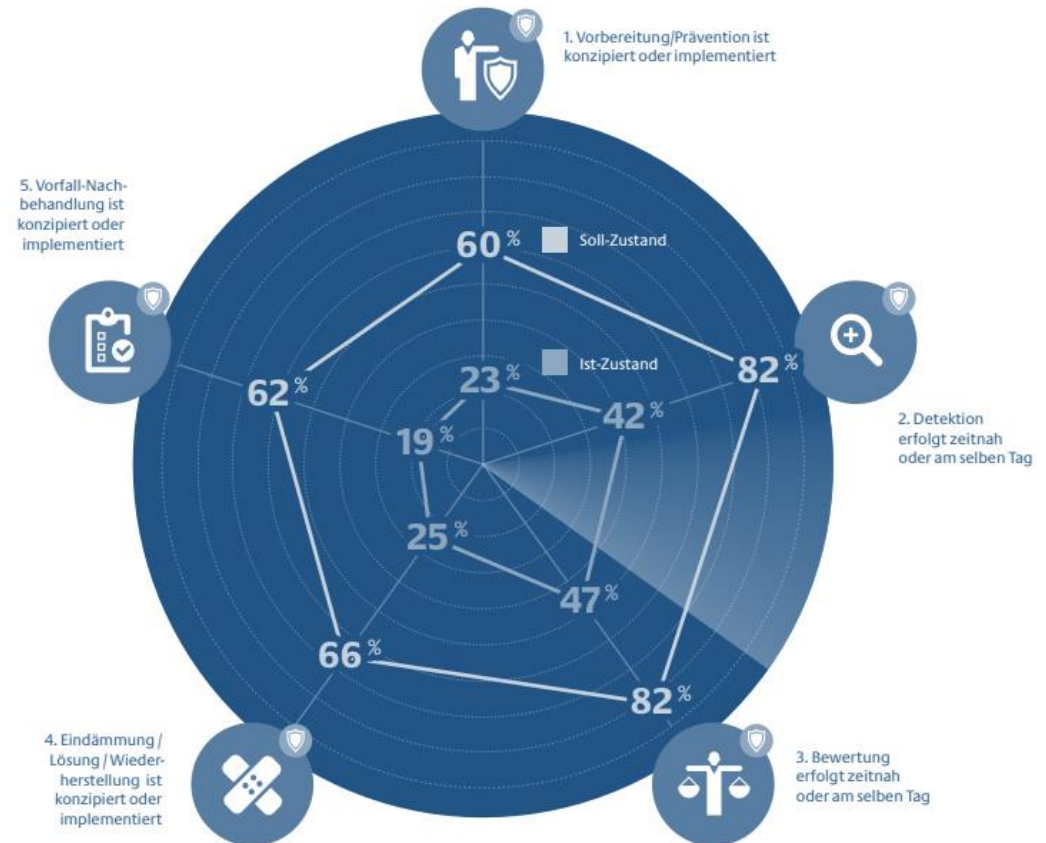
Eine Einbettung in eine Unternehmerische Routine

erscheint sinnvoll. Dabei ist das im Rahmen der Studie entwickelte Phasen Modell (vgl. ASW Bundesverband/Deloitte und Complexium) eine mögliche Guidance.

Die Ergebnisse der Expertenbefragung zeigen auch, (Achtung kleines Sample) **dass de-facto die Prozessschritte noch nicht oder unzureichend in Unternehmen implementiert sind.**

Die Phasen

1. Vorbereitung Prävention
2. Detektion
3. Bewertung
4. Eindämmung/Lösung/Wiederherstellung
5. Vorfall-Nachbehandlung



Womit müssen wir rechnen?

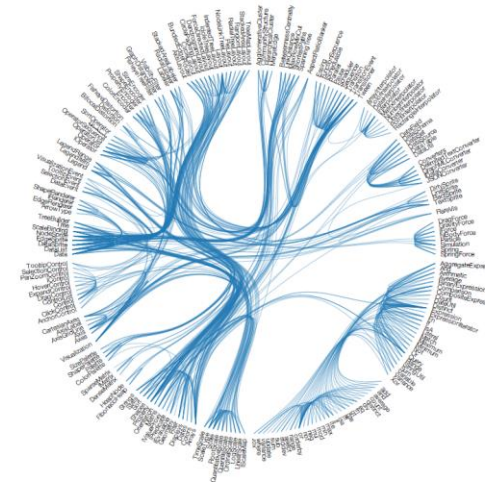
- **Fake to stay** Deep-Fakes werden künftig auch Bewegtbild realistisch manipulierbar machen.
- **Artificial Intelligence** wird die Problematik verschärfen.
- **Angriffe werden strukturierter und größer werden** und sich vermehrt gegen Unternehmen richten.
- Die **Aufklärungsarbeit ist schwierig und hat Vorlaufzeit** – dies wird so bleiben bzw. sich verschärfen.
- Wir werden mit **regulatorischen Schranken** rechnen müssen (zB. Diskussion um eine Online-ID, Fake-News Verbote), selbst wenn diese Maßnahmen nicht greifen oder bedenklich sind.

Was können wir tun?

- Klienten sensibilisieren und insbesondere **Monitoring-Kapazitäten und Frühwarnsysteme** schaffen.
- **Datenforensik und Case-Intelligence** als fixer Bestandteil unseres Portfolios.
- Aus **Bereichen lernen die das Problem länger kennen**.



Deep-Fake George W. Bush jun.



DANKE

Uwe Wolff (Naima SLS)

&

Patrick Minar (SMJ Consulting)